BİLGİSAYAR SİSTEM GÜVENLİĞİNE YÖNELİK TEHDİTLER VE TÜRKİYEDEKİ BİLGİSAYAR MERKEZLERİNDE SİSTEM GÜVENLİĞİ ÜZERİNE BİR ARAŞTIRMA

Sibkat KAÇTIOĞLU*
Üstün ÖZEN**

Özet: Bilgisayar teknolojisindeki gelişmeler bilgisayar işlemlerinin etkinlik ve verimliliğini büyük ölçüde artırırken, güvenliğin sağlanmasında da ciddi problemler ortaya çıkarmıştır. Bilgisayar teknolojisinde üstün gelişmeler sağlanırken, kasti olarak ya da kazayla, veri ve bilgiler üzerinde yapılabilecek yetkisiz değişiklik, ifşa ve tahrip gibi tehlikeler konusunda kullanıcı ve yöneticileri bilgilendirmek için yeterince çalışma yapılmamıştır. Bu çalışmayla yazılım, donanım ve veriler üzerinde yapılabilecek istenmeyen bir kısım faaliyetler hakkında kullanıcılar ve yöneticilerin bilgilendirilmesi ve bu tehditlerin oluşturduğu risklerin azaltılması için bazı pratik çözümlerin ortaya koyulması amaçlanmıştır.

I. Giriş

Bilgisayar çağının başlarında bilgisayarlar hacimce büyük ve pahalı idi. Çoklu işlemleri destekleyecek işletim sistemleri ya hiç yok veya yetersizdi. Daha sonra ağ ve dağıtılmış bilgi işlem teknolojisi karmaşık, heterojen ve yüksek ölçüde dinamik sistemler meydana getirerek, inanılmaz hızla gelişip genişlemeye başladı. Günümüzde 100 Mbps (Mega bits per second) yerel alan ağ teknolojisi halihazırda kullanılırken, gigabit (saniyede bir milyar bit) hızlarındaki teknolojinin kullanıma geçmesi çok yakındır. Dahası, terabit (saniyede bir trilyon bit) ağları üzerinde ileri araştırmalar yapılmaktadır. Bununla birlikte yeterince üzerinde durulmadığı ve önem verilmediği taktirde, yarının yüksek performanslı sistemlerinin sağlayacağı faydaları hızla kemirebilecek olan kritik bazı alanlar da ortaya çıktı. İşte sistem güvenliği, üzerinde önemle durulması gereken bu kritik alanlardan bir tanesidir. İki binli yıllara yaklaşırken sistemlerdeki gelişme hızla devam etmekte, dolayısıyla sistem güvenliği için daha dengeli ve pratik bir yaklaşım düşünülmesi gerekmektedir. Geçmişin yekpare merkezi sistemlerini korumak için kullanılan

* Prof.Dr. Atatürk Üniversitesi İİBF İşletme Bölümü
** Yrd.Doç.Dr. Atatürk Üniversitesi İİBF İşletme Bölümü

yaklaşımlar, günümüzün büyük sistemlerini desteklemek üzere geliştirilmek ve iyileştirilmek zorundadır. Güvenliğin sistemlerde etkili ve faydalı olabilmesi için güvenliğe yeni ve farklı bir bakış açısıyla yaklaşılması gerekir.

Ne olduklarını bilmeden herhangi bir tehdide karşı tedbir almak mümkün değildir. İyi bir güvenlik politikası, çok iyi bilinen tehditlere karşı aşırı reaksiyon göstermek ve az bilinen tehditlere karşı da gerektiği kadar reaksiyon göstermemek arasında bir denge kurmakta yardımcı olabilir. Her şeyin istendiği gibi güvenli kılınması mümkün olmamakla birlikte iyi bir risk politikası, tehlikenin en büyük olduğu ve güvenlik politikalarının en iyi sonuçları temin edeceği noktaları tanımlamakta yardımcı olabilir. Riskleri tam olarak değerlendirebilmek için, dört önemli unsuru göz önünde bulundurmak gerekir.

- Sisteme girip tahrip etmeye çalışanlar kimler olabilir?
- Bu kişiler neyin peşinde olabilirler?
- Aradıklarını nerede bulabilirler?
- Onları engellemek için ne yapılabilir?

Bu soruların cevabını bulabilmek için kendimizi sistemi tehdit eden kimsenin yerine koyarak onun ne yapmaya çalıştığını ve bizim o konuda ne yapabileceğimizi düşünmemiz gerekir. Güvenlik esasen tüm bilgi-işlem personelinin sorumluluğunda olan bir olaydır. Sistemin operatörleri, analistleri, programcıları ve kullanıcılarının sistemin kaynaklarını koruma ve tecavüzleri önleme hususunda kişisel sorumlulukları vardır.

Güvenlik; fiziksel, prosedürel ve teknik yönü olan bir bütündür. Bilginin ve sistem donanımının güvenliğini sağlamada hiçbir güvenlik tekniği, yalnız başına çözüm sağlamaz. Herhangi bir güvenlik programının esas maksadı yetkili kullanıcılara maksimum kullanım serbestiyetini vermekle birlikte bilgisayar kaynaklarını maksimum ölçüde korumaktır. Bunu temin etmek için fiziksel, prosedürel ve teknik kontrollerin bir kombinasyonunun seçilip uygulanması gerekir. Bunların karışımı olan bir stratejinin başarısı da neyin, hangi çerçeve içerisinde korunmaya çalışıldığına bağlıdır. Karşılaşılabilecek olan tehditler uygun bir şekilde tespit edilirse, bu tekniklerin nasıl bir karışımının kullanılacağı konusunda bir fikir geliştirilebilir.

Bilgisayar kullanımının ve ağların her geçen gün yaygınlaşmasıyla birlikte, bunlara karşı yöneltilen tehditler de artmıştır. Bilginin, bilgi kaynaklarının, ve bilgi ürünlerinin güvenilirliği günlük hayatımız ve yaşadığımız dünya için oldukça kritik bir önem arz etmektedir. Bilgisayarlarda

çok hayati ve önemli bilgiler saklanmakta ve işlenmektedir. Bu bilgilere yönelik bir tehdit, telafisi güç hatta imkansız zararlara yol açabilir. Bu yüzden, güvenlik konusu bu teknolojideki en önemli problemlerden birisi olarak karşımıza çıkmaktadır.

II. Bilgisayar Güvenliğinin Amacı

Bilgisayar güvenliğinin temel amacı, bilgi-işlem sistemlerinin ve bu sistemlerde saklanan ve işlenen verilerin gizliliğini, bütünlüğünü ve mevcudiyetini sağlamaktır. Bu üç temel fonksiyonu yerine getirebilmesi için sistemlerin yeterince güvenilir kılınması yani, sistemleri oluşturan her türlü yazılım, donanım ve verilerin çok yönlü olarak güvenliğinin sağlanması gerekir.

Güvenlik, doğru insanların doğru bilgiye erişebilmesini, bilginin doğru ve sistemin de ihtiyaç duyulduğu her an çalışır olmasını gerektirir (Schnaidt, 1992:19). Bunlara ilaveten, bir bilgisayar sistemi organizasyonun güvenlik amaçlarını da karşılamalıdır. Güvenliğin başarmaya çalıştığı en önemli amaçlardan bazıları (Goldfarb, 1992:35);

- Gizliliğin sağlanması
- Sistemin daima çalışabilirliğinin sağlanması
- Sistemin bütünlüğün sağlanmasıdır.

Bir bilgisayar sistemi, yetkisiz bir kimsenin, gizliliği olan bilgiyi görmesine izin vermemelidir. Örneğin kulak misafirliği bir sisteme nüfuz etmedeki ilk adımdır. Yani, en basit olarak görünen tehditler bile dikkate alınmadığı taktirde büyük tehditler oluşturmaya kapı açarlar (Goldfarb, 1992:35).

İdeal olarak düşünüldüğünde, bir sistem her zaman doğru çalışmalıdır. Bununla birlikte, pratikte bu mümkün olmayacaktır. Kullanıcıların bilgilere erişimi, daima tam ve zamanında mümkün olmalıdır. İşin eksiksiz yapılabilmesi için ihtiyaç duyulan tüm bilgi mevcut olmalıdır. Güvenliğin önemli bir unsuru sistemin bütünlüğünü korumak olduğu için, güvenlik tedbirleri, hem kasten hem de kazayla yapılan hataları gözlemleyecek özellikler ihtiva etmelidir. Bu alan şimdiye kadar teknik sebeplerle bu üç güvenlik özelliği içerisinde en az gelişmiş olanıdır (Morris, 1991:3).

Bütünlük, verilerin yetkisiz kişiler tarafından değiştirilmesini önlemek anlamında kullanılabilir. Bir nesnenin bütünlüğü, onun mevcut yapısı ve

orijinal ya da olması gereken yapısı kıyaslanarak değerlendirilebilir (Morris, 1991:2).

III. Bilgisayar Sistemlerinin Yüz Yüze Kaldığı Tehlikeler

Bir sistemi tam olarak güvenli kılmak hiçbir zaman mümkün değildir. Bir kimsenin geliştirmiş olduğu bir güvenlik sistemi diğer bir kimse tarafından çözülebilir. Bu sebeple, hiçbir zaman sistemin mükemmel olduğu ve zarar verilemeyeceği düşünülmemelidir. Sistemlerdeki güvenliği delmek için sayısız yollar vardır. Az bir bilgiye sahip birisi tarafından bir sisteme bağlı bir PC' ye veya başka bir sunucu bilgisayara girilebilir. Aynı şekilde, bir modem aracılığıyla sisteme bağlanılabilir. Erişim yollarının artmasına paralel olarak risk de artar.

Bilgisayar suçu çoğu zaman yüksek teknoloji gerektirmez. Bir sisteme, yetkisiz kullanıcılar tarafından fiziksel olarak ve yanlış kullanım yoluyla zarar verilebilir. Binanın içine hırsızlık amacıyla girilip hem donanım hem de veriler çalınabilir. Silindiği düşünülen önemli bilgiler yeniden bazı metotlarla geri çıkarılabilir.

Tabii felaketler her zaman olmuştur ve olmaya devam edecektir. Bazen bir şimşek çakması veya elektriğin kesilmesi bile çok kritik bilgilerin bir kısmının kaybına yol açabilir. Bütün mekanik araçlar bir yerde tıkanıklık gösterebilir veya bozulabilir. Bu durumda bir kısım değerli bilgiler de zarar görebilir.

Sistemler, diğer sistemlerle bağlantının gerçekleştiği herhangi bir noktada zarar görebilir. Bunlar aynı tip ağların birbirine bağlandığı köprülerde (bridge), veri paketlerinin adresini inceleyip bir başka ağa yönlendiren yönlendiricilerde (router) veya dijital sinyalleri analog ve analog sinyalleri de dijital sinyallere çeviren modemlerde vb. olabilir.

Sistem yöneticileri ve departman şefleri başlıca güvenlik risklerinden sayılabilir. Çünkü çoğu zaman bu kişiler, görevlerini yerine getirmeleri için gerek duydukları bilgiden daha fazlasına ihtiyaç duydukları farz edilerek gereğinden fazla yetkilerle donatılır. Örneğin, sistem yöneticisinin herkesin maaşının takip edildiği bir bordro sistemine erişiminin olması çok da gerekli olmayabilir. Veya, departman şeflerinin, emirleri altında çalışan kişilere ait her bilgiye erişmesi gerekli olmayabilir. Fakat birçok sistem yöneticisi, departman şefi veya müdür bu yönde geniş bir erişim imkanına sahiptir. Halbuki, sorumlu olmak, gereğinden fazla yetkiyle donatılmak için yeterli sebep teşkil etmez.

Bir çok kurum, kendisini iç tehditlere karşı koruma üzerinde konsantre etmiştir. Bu kurumlar çok büyük miktarlarda paralar harcayarak pahalı güvenlik yazılımları satın almakta ve hassas güvenlik sistemleri kurmaktadırlar. Halbuki bu kurumlar mevcut güvenlik sistemlerini yeterince değerlendirip kullanıcılarını eğitseler önemli miktarda para tasarruf edebilirler. Çünkü eğitimsiz kullanıcıların rakamlar üzerinde kazayla yaptıkları tahribatlar, bilgisayar sistemleri için en önemli tehlikelerden birisidir (Baker, 1995:I-2).

Kurumlar için en tehlikeli olabilecek problemlerden bir diğeri de, eskiden kurumda çalışırken herhangi bir sebeple işten uzaklaştırılan ya da işten ayrılan kişilerin yapabilecekleri tahribatlardır. Sistem yöneticiliği yapmış olanların işten ayrıldığında veya işten çıkarıldığında sistemin şifresini değiştirmesi veya bazı verileri silmeleri veyahut mevcut personelin çeşitli huzursuzluklardan dolayı sisteme virüs bulaştırmaları verilebilecek bazı örneklerdir*. Bir kişi işten çıkarıldığında veya ayrıldığında bu kişiye ait tüm kullanım hakları derhal iptal edilmelidir. Hatta bu kişilerin bilgisayarlara fiziksel olarak zarar verebileceği de göz önüne bulundurulup tedbir alınmalıdır (Daly, 1993:78).

IV. Güvenlik Teknikleri

Bilgisayar güvenliğinin sınıflandırılmasıyla ilgili olarak yapılmış farklı sınıflandırmalar mevcuttur. Bu anlamda yapılan en temel sınıflandırma fiziksel, prosedürel ve teknik güvenlik şeklindedir.

A. Fiziksel Güvenlik

Bilgisayar ya da sistem güvenliği dendiğinde akla gelen ilk şey fiziksel güvenliktir. Fiziksel güvenlik bilgisayar donanımını korumak için kullanılan cihazlar ve prosedürlere dayanır ve bilgisayar güvenliğinin en önemli yönlerinden birisidir. Diğer ofis donanımı gibi bilgisayarlar da hırsızlığa maruz kalan nesnelerdir. Fakat diğer ofis donanımının aksine bir bilgisayarın çalınmasının maliyeti, çalınan donanımın maliyetinden kat kat fazla olabilir.

---

* Amerika Birleşik Devletleri'nin Florida eyaletindeki bir gazetede çalışan bilgisayar sistem yöneticisi işten kovulduktan sonra rakip bir gazetede işe başlar. Daha önceki işvereni bir süre sonra, sadece kendi muhabirleri tarafından yapıldığını düşündükleri haberlerin, kendilerinden önce diğer rakip gazetede yayınlandığını farkeder. Araştırma neticesinde, eski sistem yöneticisin kullanım hakkının iptal edilmediği ve bu kimsenin sisteme bağlantı kurmak yoluyla haberleri çaldığını ortaya çıkarır.

Bilgisayardaki verilerin değeri bizzat bilgisayarın değeriyle kıyaslanmayacak kadar büyüktür. Nispi olarak çok pahalı olmayan bir kısım koruyucu cihazların kullanılmasıyla mevcut donanım ve içlerindeki değerli bilgilerin kaybolması veya çalınması önlenebilir (Helsing, 1987:2).

Fiziksel güvenlik tekniklerinin bir çoğu geleneksel tekniklerdir. Fakat iyi bir fiziksel güvenlik, geleneksel metotların ötesine geçmeli ve korunmaya çalışılan bilgisayar sistemi teknolojik yeniliklerle desteklenmelidir. Örneğin video kamera, insanların korumasına bir destek unsuru olarak kullanılabilir.

Fiziksel güvenlik araçları üç temel amaca hizmet eder. (Baker, 1995:87-88).

- Sistem donanımına ve verilere erişimin kontrolü. Kilitli kapılar, şifreler ve benzeri teknikler, yetkisiz kişilerin güvenlik-duyarlı alanlara girmesini engeller ve hassas bilgiye erişimi zorlaştırır.

- Bilgisayar sisteminin yerleşik olduğu alanın korunması. Yerleşimdeki temel fikir, koruma çerçevesini merkezî kısımdan dışarıya doğru genişletmektir.

- Bilgisayarlara ve muhtevasına zarar verebilecek tehlikelere karşı korunma. Bu tehlikeler, eğitimsiz ve yetkisiz insanlar tarafından kasıtsız yapılan fakat zarar unsuru taşıyabilecek teşebbüsleri ihtiva eder.

Günümüzün bilgisayar sistemlerinde güvenlik, sistemi merkezi bir yerde kilitlemek suretiyle sağlanamaz. Fakat merkezi işlem birimini veya sunucu bilgisayarı kilitli kapılar arkasında muhafaza etmek iyi bir yol olabilir. Sistemin diğer elemanları, bir binaya, bir fabrika yüzeyine, bir ülkeye ve hatta dünyaya yayılabilir. Artık fiziksel erişimi önleme gayretleri tek bir işletim yüzeyi ile sınırlanamaz. Bilgisayarların hacimce ve fonksiyonca gelişmesiyle birlikte, güvenliği sağlama işi daha zor bir hale gelmiştir. Büyük ihtimalle, yakın zamanda bilgisayar sistemlerinin temel elemanları, telefon sisteminin temel elemanlarından ayırt edilemeyecek duruma gelecektir. Bu durum, bilgisayar sistemini daha fazla zarar verilmeye müsait hale getirecektir.

Yeni bilgi kaydetme yolları ve araçları fiziksel güvenlik için yeni tehlikeleri de beraberinde getirmektedir. Disketler buna basit bir örnektir. Sekiz inçlik çapla başlayan disketler daha sonra beş ince ve nihayet üç buçuk ince kadar küçülmüş, dolayısıyla binlerce sayfalık değerli bilgiyi disket veya CD' lerle bir cepte veya çantanın bir köşesinde gizlemek mümkün hale gelmiştir. Bilgi kaydetme araçlarının saklandığı iyi korunmayan bir yerden bu araçları çalmak zor bir iş değildir.

Bir fiziksel güvenlik sistemi, sistem donanımını koruduğu kadar bilgileri de korumalıdır. Bilgileri korumanın belki de daha önemli olduğu söylenebilir. Bazen bilgileri çok yüksek teknoloji gerektirmeyen yollarla kaybederiz. Çöpe atılan yazıcı çıktıları ve bilgisayar monitörüne yapıştırılmış veya yazılıp çekmeceye bırakılmış bir şifre bunun en basit örnekleridir. Fiziksel güvenlik tekniklerinin çoğu şu özellik etrafında bina edilmiştir: yetkili kişileri kabul, yetkili olmayanları ret. Bu farkı ortaya koymanın üç yolu vardır (Schwartau, 1995:52).

1. Bir şifre, daha karmaşık bir erişim kodu veya basit bir tanımlayıcı kullanmak.
2. Bir elektronik kart veya tanımlayıcı bir rozet kullanmak.
3. Parmak izi, ses özellikleri veya bir imza gibi biyolojik özellikleri test etmek.

Yaygın olarak kullanılan fiziksel güvenlik teknikleri Tablo 1'de verilmiştir.

Tablo 1: *Fiziksel Güvenlik Teknikleri*

Teknikler	Özelliği
Sigara içmenin ve yemek yemenin yasaklandığı alanlar	Olması gerekli
Bilgisayar güvenlik görevlisi (Bu pozisyonu gerekli kılacak derecede kaynakları olan organizasyonlar için)	İsteğe bağlı
Elektriksel donanımın korunması	Olması gerekli
Güç kesintisine karşı önlemler	Olması gerekli
Evrak trafiğinin yoğun olduğu durumlarda gelen ve giden materyallerin yoklanması	İsteğe bağlı
Hassas üretim hizmetlerinin izolasyonu	Olması gerekli
İş alanlarındaki trafiğin ve erişimin en düşük düzeyde tutulması	Olması gerekli
Terminallerden erişim için şifre kullanımı	Olması gerekli
Fiziksel erişim bariyerleri	Olması gerekli
Uzaktaki terminallerin fiziksel güvenliği	Olması gerekli
Manyetik teyp kullanımı fazla olduğunda etiketleme yönetimi	İsteğe bağlı
Ziyaretçi trafiğinin yoğun olduğu ve çok fazla personelin çalıştığı durumlarda evrensel nitelikte kimlik belirleyici kartların kullanımı	İsteğe bağlı
Terminaller ve iş istasyonları üzerinde bazı sınırlamalar koyulması	Olması gerekli

Kaynak: Baker, Richard H., Network Security:How to Plan for It and Achieve It, s. 109.

B. Prosedürel Güvenlik:

Gerektiği gibi kullanılmadığı taktirde en iyi fiziksel ve teknik metotların bile çok fazla bir değeri yoktur. Güvenlik, bilgilerin yetkisiz ifşa, hasar, tahrip ve değişikliklere karşı korunması ve kontrol edilmesi için gerekli idari politika ve prosedürlerle de desteklenmelidir. Prosedürel kontroller, verilerin girilmesi, değiştirilmesi veya kullanılması esnasında dikkat edilecek kurallardan ibarettir. Bu koruma ve kontrol, bilginin nasıl proses edileceğini, nasıl dağıtılacağını, nasıl kaydedileceğini ve gerektiğinde nasıl tahrip edileceğini ihtiva eder ve kasıtlı veya kasıtsız olarak yapılabilecek yanlış veri girişlerine karşı önlem almak için kullanılır.

Tablo 2: *Prosedürel Güvenlik Teknikleri*

Teknikler	Özelliği
Veri kullanım sorumluluğunun kullanıcılara verilmesi	Olması gerekli
Bilgisayar güvenliği yönetim komitesi oluşturulması	Olması gerekli
Bilgisayar sistem faaliyetlerine ilişkin kayıtların tutulması	Olması gerekli
Bilgisayar erişim kontrolünün yönetimi	Olması gerekli
Bilgisayar güvenlik görevlileriyle işbirliği içerisinde çalışılması	Olması gerekli
Kuryelerin güvenilirliliğinin sağlanması	İsteğe bağlı
Verilerin hassasiyet seviyesine göre sınıflandırılması	İsteğe bağlı
Veri dosyalarının ve programların yedeklenmesi	Olması gerekli
İşe yaramayan ya da kullanılmayan materyallerin yok edilmesi	Olması gerekli
Elektronik bilgi işlem denetimin yapılması	İsteğe bağlı
Finansal kayıp durumunda zararı karşılamak için sigorta yapılması	Olması gerekli
Denetimcilerin bağımsız bir şekilde bilgisayar kullanımının sağlanması	İsteğe bağlı
Güvenlik raporlarının gizli tutulması	Olması gerekli
Manyetik teyp bakımının yapılması	Olması gerekli
Hassas raporların kopyalarının en az sayıda tutulması	Olması gerekli
Erişimin sınırlandığı durumlarda bilgisayar kullanımının izlenmesi	Olması gerekli
Terminal erişimlerinde şifrelerin kullanılması	Olması gerekli
Hassas dokümanlar üzerinde ikazlar koyulması	İsteğe bağlı
Hassas veri dosyaları ve program isimlerinin gizliliğinin sağlanması	İsteğe bağlı
Hassas bölgelerin güvenliğinin sağlanması	Olması gerekli
Eksik ve eski verilerin tamamlanması veya güncelleştirilmesi	Olması gerekli

Kaynak: Baker, Richard H., Network Security:How to Plan for It and Achieve It, s. 128-129.

Prosedürel kontrollerin etkin bir şekilde kullanımıyla güvenlik tedbirlerinin sistemin tam ve etkili kullanımına zarar verme derecesi minimize edilebilir. Prosedürel güvenlik kontrolleri tüm güvenlik işlemlerini kapsadığı iç in, organizasyonun vazgeçilmez bir parçası konumundadır. Prosedürel metotlar, fiziksel ve teknik kontrolleri destekledikleri ve uygun çalışma düzeninin sağlanmasına yardım ettikleri için özellikle önemlidir. Hangi güvenlik metodu seçilirse seçilsin, bu metotların etkinliği, veri, donanım ve personel üzerinde ne derece iyi ve devamlı kontroller uygulandığına bağlıdır (Shaffer ve Simon, 1994:77-78). Prosedürel tekniklerin en önemlileri Tablo 2' de verilmiştir.

C. Teknik Güvenlik:

Teknik güvenlik, programlara ve verilere erişimi kontrol etmek ve işletim sisteminin gerektiği şekilde fonksiyon görmesini sağlamak için kullanılan donanım kontrolleri, kullanıcıları tanımlamak ve erişimlerini kontrol etmek için kullanılan yazılım kontrolleri ve iletişim sisteminin bileşenlerinin kullanımını düzenleyen iletişim kontrollerinden oluşur.

Bilgisayar sistemlerinin ve kişisel bilgisayarların gittikçe artan bir şekilde yaygınlaşarak kullanılması teknik güvenlik konusunun daha dikkatli bir şekilde ele alınmasını zorunlu hale getirmiştir. Bir bilgisayar sisteminin yapısı bu tür güvenliği gerekli kılmaktadır. Fiziksel koruma günümüz sistemlerinde eski merkezi sistemlere oranla çok daha zor bir hale gelmiştir. Günümüzde eskiye oranla çok fazla sayıda kullanıcı mevcuttur. Bir zamanlar insanların çok az bir kısmı bilgisayarların nasıl kullanıldığını bilmekte iken günümüzde nasıl kullanıldığını bilmeyenler azınlıkta kalma yolundadır. Bu nedenle prosedürel kontrollerle bir sistemi yönetmek son derece zor bir hâle gelmiş ve sistem güvenliğinin gerektiği şekilde sağlanması için teknik kontrollerin uygulanması önem kazanmıştır. Bilgisayar sistemlerine karşı yapılan çoğu tehdit ve tacizlere karşı korunabilmek için bugün çok sayıda teknik tedbir mevcuttur (Department of Trade and Industry, 1991:132). Önemli bazı teknik kontroller Tablo 3' de verilmiştir.

Tablo 3: *Teknik Güvenlik Teknikleri*

Teknikler	*Özelliği*
Bilgisayar programı değişiklik izleme raporları	Olması gerekli
Şifre dosyası enkripsiyonu	Olması gerekli
Bilgisayar kullanımı erişim kontrol yönetimi	Olması gerekli
Veri dosyalarına erişim kontrolü	Olması gerekli
Veri dosyaları ve programların yedeklenmesi	Olması gerekli
Terminal erişimi için şifre kontrolü	Olması gerekli
Özel bilgilerin görüntülenmesinde sınırlamalar	Olması gerekli
Sistemi test etmede kullanılan verilerin korunması	Olması gerekli
İhtiyaçlar belirlenmesinde denetimcilerin katkısı	Olması gerekli
İşletim sistemindeki değişikliklerin teknik bir yaklaşımla gözden geçirilmesi	Olması gerekli
Satıcı tarafından sağlanan program bütünlüğü ve güvenlik özellikleri	Olması gerekli
Veriler için çok fazla korumaya ihtiyaç duyulduğu ve özellikle ağ üzerinde çalışıldığı zaman enkripsiyon uygulaması	İsteğe bağlı
Verilerin hassaslığı değişken olduğu durumlarda veri sınıflandırması	İsteğe bağlı
Kullanıcı tarafından dinamik şifre değiştirme kontrolü	İsteğe bağlı
Bilgisayar kullanımının izlenmesi.	İsteğe bağlı
Otomatik şifre üretimi	İsteğe bağlı
Hassas bilgiler ihtiva eden dosya isimlerinin gizliliği	İsteğe bağlı

Kaynak: Baker, Richard H., Network Security:How to Plan for It and Achieve It, s. 147-148.

V. Bilgisayar Sistem Güvenliğinin Türkiye'deki Durumu

Bu çalışmada, Türkiye'de bilgisayar sistem güvenliği konusunun ne derece hassasiyetle ele alındığını, bugüne kadar geliştirilmiş olan tekniklerin ne derece takip edilerek uygulamaya koyulduğunu, hangi tekniklerin yaygın olarak kullanıldığını ve ideal anlamda bir güvenlik sistemi oluşturulması yönünde nelerin yapılabileceğini tespit etmek amacıyla güvenlik, fiziksel, prosedürel, teknik ve şifre güvenliği açısından; ayrıca kişisel bilgisayar tabanlı sistemler için de yukarıdaki başlıklara ilaveten, kötü niyetli yazılımlar açısından bir araştırma yapılmıştır.

Araştırmada sistem güvenliğini çeşitli yönlerden inceleyen 32 sorudan müteşekkil bir anket formu kullanılmıştır. Soruların bir çoğu, sıralanan çok sayıda seçenekten ilgili kısımlarının işaretlenmesi esasına dayalı, bir kısmı çoktan seçmeli, bir kısmı da "evet-hayır" şeklindeki sorulardır.

Soruların hazırlanmasında, Richard A. Baker'ın "Network Security: How to Plan For It And Achieve It" isimli kitabının Appendix A kısmındaki "Eighty-two Control Tactics Analyzed" başlığı altında sıralanan güvenlik kontrol taktikleri esas alınmıştır. Bu teknikler orijinal olarak, Amerikan Adalet Bakanlığı, Adalet İstatistikleri Bürosu (U.S. Department of Justice, 1982) tarafından hazırlanan Bilgisayar Güvenlik Teknikleri isimli rapordan alınmıştır. Çalışmada kullanılan diğer bir çok kaynaktan gerekli görülen bazı tekniklerin ilavesiyle sorular zenginleştirilmiştir.

Araştırmada şansa bağlı kota örneklemesi yapılmıştır. Bankacılık, sigortacılık, otelcilik, nakliyecilik, sağlık, savunma, adalet, üniversite, imalat ve hizmet gibi bir çok sektörden kurum seçilmiştir. Kamu sektöründeki büyük kurumların önemli bir kısmı araştırmaya dahil edilmiştir. Bu kurumların bir çoğu, kâr amaçlı olmayan hizmet kurumlarıdır.

Araştırma uygulanan kurum sayısı 69' dur. Bu kurumlardan 37'si kamu, 32'si ise özel kurumdur. Bu, yaklaşık %53.6 kamu, %46.4 özel kurum yüzdesine karşılık gelmektedir. Görüşme yapmayı planladığımız yaklaşık 6 kurum görüşme talebimizi geri çevirerek, bu konunun hassas bir konu olduğunu dolayısıyla bize yardımcı olamayacaklarını ifade etmişlerdir.

Araştırma, anket formunun, anket uygulanan kurumların bilgi-işlem müdürleri, bilgi-işlem müdür yardımcıları, sistem yöneticileri gibi uzman kişilerle yüz yüze görüşmeler yapılarak doldurulması suretiyle gerçekleştirilmiştir. Araştırmada yüz yüze görüşme tekniği kullanıldığı için bilgi-işlem merkezleri bizzat ziyaret edilerek incelenmiş, dolayısıyla araştırmada eksik kalabilecek bazı noktaların takviye edilmesi mümkün olmuştur. Görüşmenin başlangıcında bu çalışmanın akademik amaçlı bir çalışma olduğu, bu bağlamda elde edilecek sonuçların kendileri açısından da önemli olduğu, ayrıca sonuçlar değerlendirilirken kurum bazında değerlendirilme yapılmayacağı, değerlendirmenin genel olacağı söylenerek cevaplarda objektif kalınması temin edilmiştir. Cevaplayıcılar için sorularda kapalı kalabilecek noktalar izah edilerek hatalı cevaplar verilmesi önlenmeye çalışılmıştır. Yapılan mülakatlarda notlar alınarak bunlar daha sonra değerlendirilmeye tabi tutulmuştur. Sonuç olarak, araştırma, anket, gözlem ve mülakat metotlarının bir kombinasyonu şeklinde cereyan etmiştir.

Anket uygulanan kurumların sistemleri küçük, orta ve büyük olmak üzere üç kategoriye ayrılmıştır. Bu kategoriler belirlenirken, işletim sistemlerinden, sistemlerin dağıtılmış olma ölçülerinden ve bizzat kurumların özelliklerinden hareket edilmiştir.

Küçük sistemler, genel olarak yerel alan ağlarından oluşmaktadır. Bu kategoride değerlendirilen sistemler sadece yerel alan ağına sahip olan kurumlar için söz konusudur. Çünkü bir kurum aynı anda hem yerel alan ağına hem de büyük sistemlere sahip olabilir. Bu kategori içerisindeki sistemleri kullanan kurumlar, hastaneler, oteller, nakliye firmaları, bazı holdingler ve bazı kâr amaçlı olmayan kamu hizmet kuruluşlarıdır.

Orta sistemler genellikle ana bilgisayar (mainframe) türünde ve az dağıtılmış sistemlerdir. Bu sistemlere sahip olan kurumlar daha çok kâr amaçlı olmayan kamu kurumları, bakanlıklar ve askeri kurumlardır.

Büyük sistemler, yüzlerce şubeye (yurt içi-yurt dışı) hizmet veren bankaların, sosyal güvenlik kurumları ve büyük imalat şirketlerinin sahip oldukları ağlardır. Bu merkezler, yerel alan ağlarını, ana bilgisayar ve büyük ağları aynı anda uhdesinde bulundurmaktadır.

Sonuçların değerlendirilmesinde deskriptif istatistiklerden ve çeşitli tekniklerin kullanılmasının sistem büyüklükleri itibariyle bir fark gösterip göstermediğinin tespiti amacıyla χ^2 -kikare- testinden yararlanılmıştır. Bu amaçla SPSS* isimli bir paket program kullanılarak analizler gerçekleştirilmiştir. Sosyal bilimlerde yaygın olarak kullanılan 0.05 lik güven düzeyi esas alınmıştır.

V. Bulgular

• Sistem güvenliğinin Türkiye'deki durumunu tespit etmek amacıyla yapmış olduğumuz uygulamayla aşağıda sıraladığımız sonuçlar elde edilmiştir. Anket soruları ve değerlendirme sonuçları Ek.1' de verilmiştir.

• Bilgi-işlem merkezlerinin çok büyük bir kısmında, en önemli fiziksel tedbir olarak düşünülen sistem odasına fiziksel erişimi önleme konusunda teknolojik imkanlardan yararlanılmadığı görülmektedir. Çok büyük paralar harcanarak kurulan ve sistem donanımının fiyatıyla dahi kıyaslanmayacak ölçüde önemli bilgiler ihtiva eden sistemlerin fiziksel olarak güvenliği, sistemlerin bulunduğu alanlara erişimin mümkün olduğu kadar zorlaştırılmasıyla önemli ölçüde başarılabilir. Günümüzde oldukça yaygınlaşan

---

* SPSS, Statistical Package for Social Sciences, çok kapsamlı bir istatistiksel analiz paket programı olup tüm dünyada yaygın olarak kullanılmaktadır. Bu çalışmada SPSS for Windows' un 5.0.1 sürümünden faydalanılmıştır.

ve fiyatları da nispeten ucuzlayan çeşitli teknolojiler mevcuttur. Sistem alanlarına fiziksel erişimi engellemek için en fazla tercih edilen sistemler kartlı sistemlerdir. Araştırma, biyolojik özellikleri test eden biyometrik teknik kullanımının Türkiye'de henüz olmadığı ortaya koymuştur. Bununla birlikte, yakın zamanda yaygınlaşması beklenen biyometrik tekniklerin, özellikle çok büyük merkezler tarafından kullanılması mümkün olabilecektir .

• Sistem alanının kameralarla izlenmesi, su geçirmez tavanlar, bilgisayar merkezlerine giren çıkan materyallerin kontrolü, bina girişlerine turnike, muhafız vb. fiziksel engeller konulması ve alarm cihazları en az uygulanan fiziksel kontroller olarak ortaya çıkmaktadır.

• Yangınlar bütün maddi varlıklar için olduğu gibi bilgisayar sistemleri için de potansiyel bir tehlike kaynağıdır. Kasıtlı veya kasıtsız olarak sistemlerin yangınlara maruz kalması mümkün olabilir. İncelediğimiz bilgi-işlem merkezlerinin tamamına yakını herhangi bir şekilde yangınlara karşı tedbir almıştır. Yalnız, sistemlerin yaklaşık dörtte birinde yangınlara karşı alınan tedbirlerin sadece yangın söndürme aletlerine münhasır kalması ilginçtir. Araştırma, aynı zamanda teknolojik bir yenilik olan otomatik yangın söndürme sistemlerinin gittikçe daha yaygın bir şekilde kullanılmaya başlandığını da ortaya koymuştur.

• Sistemlerde yaşanan olumsuzlukların çoğu mekanik arızalardan kaynaklanmakta fakat bu arızaların önlenmesi de mümkün gözükmemektedir.

• Sistemlerde yapılan ve donanımda hasar ya da bilgi kaybına sebep olan hataların yarıdan fazlası insan unsurundan kaynaklanırken yarıya yakını da bizzat sistemlerin kendisinden kaynaklanmaktadır. İnsan unsurundan kaynaklanan hataları önlemenin yolu güvenlik eğitimidir.

• İncelediğimiz bilgi-işlem merkezlerinde doğal afetlerden kaynaklanan bir zarar ya da bilgi kaybı söz konusu değildir. Ancak bu durum, doğal afetlerin bu sistemler için hiçbir zaman tehlike oluşturmayacağı anlamına gelmez. Dolayısıyla, potansiyel bir tehlike kaynağı olarak düşünülerek gerekli tedbirler alınmalıdır.

• Yerleşim yeri güvenliği konusunda bilgi-işlem merkezleri istenen seviyede değildir. Çünkü sistemlerin sadece iki tanesi bu amaçla tasarlanmış binalarda kurulmuştur. Bilgi-işlem merkezlerinin büyük çoğunluğu, bağlı oldukları kurumların genel merkezlerinin bulunduğu binaların nispeten uygun olan bir katı seçilerek kurulmuştur. Bu nedenle yerleşim yerinin güvenli kılınması sınırlı kalmaktadır. Bilgi-işlem merkezlerinde personel trafiği için

ayrı, acil durumlar ya da bilgisayar donanımının taşınması için de ayrı olmak üzere iki adet giriş-çıkış bulunması tavsiye edilmesine rağmen, araştırılan merkezlerin sadece dörtte birinde bu uygulamayla karşılaşılmıştır. Merkezlerin yaklaşık dörtte üçü sadece bir giriş-çıkışa sahiptir. Bu tür uygulamaların yapılabilmesi için, kurumların sistemlerini kurarken özel bina tasarlamaları gerekmektedir. Aksi taktirde, bu uygulama hiç bir zaman istendiği şekilde gerçekleşemeyecektir.

• Prosedürel anlamda alınması gereken tedbirlerin yaygın olarak kullanıldığı söylenebilir. Bununla birlikte, kurye güvenilirliğinin testi, verilerin hassasiyet seviyesine göre sınıflandırılması ve manyetik teyp veri tabanı bulundurulması şeklinde belirtilen prosedürel tedbirlerin uygulamasının düşük olduğu görülmektedir.

• İncelediğimiz bilgi-işlem merkezlerinin tamamına yakını çalıştıracakları personelin işe alımında ve sonrasında çeşitli kontroller uygulamaktadır. Fakat bu anlamda en önemli kontrol olarak nitelenebilecek olan, işten ayrılan personelin kullanım haklarının iptali, merkezlerin yaklaşık üçte birinde yapılmamaktadır. Kuruma kızgın bir şekilde işten ayrılan ya da işten atılan bir personelin, üstelik yetkili bir kullanım hakkına sahipse, uzaktan erişim vasıtasıyla telafisi güç hatta imkansız zararlar vermesi, ancak bu hakkın derhal iptal edilmesi ya da şifrelerinin değiştirilmesiyle önlenebilir.

• Kurumların sadece üçte biri sistem güvenliği konusunda kullanıcılarını herhangi bir şekilde eğitmektedir. Gerçekte formal bir güvenlik programı uygulayan bilgi-işlem merkezi sayısı yok denecek kadar azdır. Halbuki eğitim, güvenlik konusunda kullanıcıları bilgilendirmenin en önemli yoludur. Aksi taktirde kişiler bunu yaşayarak öğreneceklerdir ki bu da pahalı bir deneyim olabilir.

• Teknik kontrollerden bilgisayar güvenliği açısından önemi en az anlaşılan tekniğin enkripsiyon uygulaması olduğu söylenebilir. Bunun sebebi ya bu sistemlerde tutulan bilgilerin korunmaya değmeyecek kadar önemsiz olması ya da bu bilgilerin herhangi bir tehdide maruz kalmayacağı konusunda bir kaygı taşınmamasıdır. Sistemlerin yaklaşık yüzde doksanı enkripsiyon kullanmamaktadır. Yüzde altmışa yakını ise şifre dosyasını bile enkript etmeksizin saklamaktadır.

• Şifre yönetimi geleneksel olarak alışılagelmiş metotlarla yapılmaktadır. En başta, şifreler oluşturulurken ya kullanıcılara sorulmakta veyahut ta sistem yöneticisi tarafından verilmekte, bilgisayarlara rasgele şifreler

ürettirme yoluna gidilmemektedir. Bilgi-işlem merkezlerinin yarısından fazlası hassas şifreleri periyodik bir esasa bağlı olarak değiştirmemektedir. Halbuki şifreler tahmin edilme veya çalınma ihtimaline karşı sık aralıklarla değiştirilmelidir. Araştırma, yetkisiz kimselerin şifreleri tahmin etmek için sürekli login denemesi yapmasını engellemek amacıyla uygulanması gereken login sınırlamalarından hiçbirisinin, sistemlerin yüzde kırkı tarafından uygulanmadığını ortaya koymuştur. Bu durum, şifrelerin çalınması ve dolaysısıyla sistemin ve bilgilerin taciz edilmesine davetiye çıkarmaktadır.

• Araştırmamız virüslerin sistemler için önemli bir tehlike kaynağı olduğunu bir kez daha ortaya koymuştur. Çünkü araştırılan bilgi-işlem merkezlerinin yaklaşık olarak yarısının virüslerle başlarının derde girdiği ortaya çıkmıştır. Virüslerin en çok korkulan tarafı olan bilgilerin tahrip edilmesi, virüs problemi yaşayan merkezlerin büyük çoğunluğunun başına gelmiştir. Diğer bir ilginç sonuç da, incelenen bilgi-işlem merkezlerinin dörtte birinin virüslere karşı herhangi bir şekilde tedbir almadıklarıdır. Araştırma, anti-virüs yazılımlarının virüslerin tespiti ve ortadan kaldırılmasında en yaygın yol olduğunu da ortaya koymaktadır. Virüslere karşı tedbir aldığını belirten merkezlerin tamamına yakını anti-virüs yazılımlarından faydalanmaktadır. Ayrıca virüslerle mücadelede eğitime, çok önem verilmemektedir.

• Araştırmanın ortaya koyduğu diğer bir önemli sonuç da bilgi-işlem merkezlerinin büyük çoğunluğunun sistemlerinde lisanssız ve kopya programlar kullanıyor olmalarıdır.

• Önemli bazı fiziksel tekniklerin kullanımı sistem büyüklükleri itibariyle önemli bir farklılık göstermemektedir. Sadece sistem alanlarına girişte büyük sistemlerin çok büyük bir kısmı çeşitli teknolojiler vasıtasıyla tedbir alırken, küçük ve orta sistemlerin tamamına yakını herhangi bir teknoloji kullanmamaktadır. Fiziksel tedbirlere benzer şekilde, sistem büyüklükleri itibariyle prosedürel kontrollerin uygulanması bakımından da genelde önemli farklılıkların bulunmadığı sonucu çıkmıştır. Fiziksel ve prosedürel kontrollerin aksine, teknik kontrollerden bir çoğunun uygulanması sistemler itibariyle farklılık göstermiştir. Dolayısıyla, teknik tedbirlerin büyük sistemlerde kullanımının daha yaygın olduğu söylenebilir. Yangına karşı alınan önemli tedbirler, sistem büyüklükleri itibariyle önemli farklılıklar göstermektedir. Büyük sistemlerde yangına karşı alınan tedbirler konusunda küçük sistemlere oranla çok daha hassas hareket edilmektedir.

• Bilgisayar güvenlik tekniklerinin çok büyük bir kısmının uygulanmasında sektörler itibariyle belirgin bir farklılık görünmemektedir.

Karşılaştırma yapılan çok sayıda teknik içerisinden sadece çalışma saatleri haricinde alarm sistemleri kullanılması, bilgisayar sistemlerinin yerleşim yeri ve personel alımlarında referanslar alınıp kontrol edilmesi hususlarında kamu ve özel sektör arasında bir farklılık müşahede edilmiştir. Buna göre bu üç konuda da özel sektör sistemleri daha iyi durumdadır. Sonuçlara genel olarak bakıldığında hemen hemen tüm tekniklerin uygulanmasında özel sektör lehine çok küçük nispi farklar müşahede edilmiştir.

VI. Sonuç

Sonuç olarak, ne kadar kontrol uygulanırsa uygulansın, hangi tedbirler alınırsa alınsın, bilgisayar sistemleri için mükemmel anlamda bir güvenlik sağlamanın mümkün olmayacağı söylenebilir. Çünkü bir insan aklının geliştirmiş olduğu bir teknik, diğer bir insan aklının geliştirmiş olduğu başka bir teknikle aşılabilir. Bir duvar ne kadar yüksek yapılırsa yapılsın onu aşacak merdiven de yapılabilir. Bu demek değildir ki, korunma yapılmamalıdır. Hiç bir güvenliğin olmaması sistemde herkesin her istediğini yapması, tam güvenlik ise hiç kimsenin hiç bir şey yapamaması demektir. Güvenlik, sistemi kullananların yapmaları gereken işlerini icra etme kabiliyetlerini olumsuz etkilemeksizin, verileri ve bilgisayar donanımını kasıtlı veya kasıtsız yapılan tehditlere karşı korumalıdır.

Summary: Advances in computer technology have greatly improved efficiency and effectiveness of the computer operations but, also presented some serious problems in achieving adequate security. While excellent progress has been made in computer technology, very little has been done to inform users and managers about such threats as unauthorized modification, disclosure, and destruction of data and information, either deliberate or accidental. This study is aimed to make users and managers aware of some of the undesirable actions that can happen to hardware, software and data and provide some practical solutions for reducing risks to these threats.

Kaynaklar

Baker, Richard A., **Network Security:How to Plan for It and Achieve It.**, McGraw-Hill, Inc., New York, 1995.

Daly, James, "***Out to Get You***," Computerworld, March 22, 1993.

Department of Trade and Industry, **Information Technology Security Evaluation Criteria (ITSEC)**, London, June 1991.

Goldfarb, Michael G., "*A **Password to Computer Security***," Financial Executive, July/August 1992.

Helsing, Cheryl, **Computer User's Guide to the Protection of Information Resources**, The National Institute of Standards and Technology(NIST) Computer Security Program Office, A-216 Technology, Gaithersburg, 1987.

Morris, Gary S., **Computer Security and Law**, GSM Associates, Suite 202, Falls Church.

Schwartau, Winn, "***New Keys to Network Security***," Infoworld, May 15, 1995.

Shaffer, Steven L., Alan R. Simon, **Network Security**, Academic Press, Cambridge, 1994.

Statistical Package for Social Sciences (SPSS^{X}) User Guide (SPSS for Windows), McGraw-Hill, Inc, New York, 1992.

U.S. Department of Justice, **Bureau of Justice Statistics, Computer Security Techniques**, Government Printing Office, Washington, DC, 1982.

EK 1: *Anket Soruları Değerlendirme Sonuçları*

Sorular ve Seçenekler	*Frekans*	*Nispi Frekans (%)*
1.Sisteme odasına girişte kullanıcıları nasıl ayırıyorsunuz?		
• Şifre, kişisel tanıtım kodu vb. bilgilere bağlı olarak.	5	7.2
• Kimlik kartı, manyetik kartlar, rozetler vb araçlarla	21	30.4
• Parmak izi, ses, imza vb. gibi biyolojik özellikleri test eden biyometrik tekniklerle	0	0.0
• Hiçbiri	42	60.9
• Diğer (Belirtiniz)	1	1.4

2. Fiziksel güvenliği temin etmek üzere uyguladığınız teknikleri işaretleyiniz.	Frekanslar		Nispi Frekanslar (%)	
	Evet	Hayır	Evet	Hayır
• Sigara içilmesi ve yemek yenilmesinin yasaklandığı alanlar	45	24	65.2	34.8
• Sistem alanının kameralarla izlenmesi	6	63	8.7	91.3
• Bilgisayar güvenliğinden sorumlu elemanların bulundurulması	37	32	53.6	46.4
• Su geçirmez donanım örtüleri ve tavanlar	7	62	10.1	89.9
• Güç kesintisine karşı güç kaynakları	67	2	97.1	2.9
• Elektrik donanımının korunması	41	28	59.4	40.6
• Giren-çıkan materyallerin yoklanması	12	57	17.4	82.6
• Sisteme fiziksel erişimi engellemek için turnike benzeri bariyerler kurulması	21	48	30.4	69.6
• İmzalı giriş-çıkış takipleri	9	60	13.0	87.0
• Emniyetli ısıtma, soğutma ve havalandırma sistemleri	61	8	88.4	11.6
• Merkezi işlemci, yazıcı vb. teçhizatın müstakil odalarda bulundurulması	59	10	85.5	14.5
• Çalışma saatleri haricinde sistem odasına yetkisiz girişi önlemek için alarm cihazları	11	58	15.9	84.1
• Diğer.(Belirtiniz)	2	67	2.9	97.1
3. Yangın ihtimaline karşı ne tür tedbirleriniz var?				
• Yangın alarmları	40	29	58.0	42.0
• Yangın söndürme aletleri	56	13	81.2	18.8
• Yangına dayanıklı malzemeler	10	59	14.5	85.5
• Duman ya da ısı detektörleri	37	32	53.6	46.4
• Otomatik yangın söndürme sistemleri	27	42	39.1	60.9
• Hiçbiri	2	67	2.9	97.1
• Diğer.(Belirtiniz	0	69	0.0	100.0

EK-1: *Anket Soruları Değerlendirme Sonuçları (devam)*

Sorular ve Seçenekler	*Frekanslar*		*Nispi Frekanslar(%)*	
	Evet	*Hayır*	*Evet*	*Hayır*
4. Sisteminizde aşağıdaki olumsuzluklardan hangilerini yaşadınız?				
• Harici elektrik kaynaklarından gelen karışıklık (voltaj yükselmesi ve düşüklüğü	20	49	29.0	71.0
• Güç kaynağında meydana gelen arızalar	36	33	52.2	47.8
• Gaz, su vb. tesisatlarda patlamalar.	6	63	8.7	91.3
• Mekanik arızalar	28	41	59.4	40.6
• Yangın	0	69	0.0	100.0
• Sabotaj	0	69	0.0	100.0
• Donanım hırsızlığı	1	68	1.4	98.6
• Hiçbiri	18	51	26.1	73.9
• Diğer.(Belirtiniz)	2	67	2.9	97.1
5. Hata sonucu sisteminizde herhangi bir hasar ve/veya bilgi kaybı meydana geldi mi?	19	50	72.5	27.5
6. Yukarıdaki soruya cevabınız "evet" ise nedeni?				
• Yazılım, konfigürasyon ve kuruluş hataları	0	19	0.0	100.0
• Kullanıcı hataları	8	11	42.1	57.9
• Operatör hataları	3	16	15.8	84.2
• Veri hazırlama hataları	0	19	0.0	100.0
• Çıkış hataları	0	19	0.0	100.0
• Sistem hataları	12	7	63.2	36.8
• Haberleşme hataları	0	19	0.0	100.0
• Diğer.(Belirtiniz)	3	16	15.8	84.2
7.Doğal afetler sebebiyle sisteminizde bir hasar ve/veya bilgi kaybı meydana geldi mi?	0	69	0.0	100.0
10.Aşağıdaki kimlik belirleyici kartların hangileri sistem odasına ya da güvenli alanlara girişte kullanılıyor?				
• Pasif elektronik kodlu kimlik kartları	1	68	1.4	98.6
• Aktif elektronik kimlik kartları	9	60	13.0	87.0
• Matematiksel fonksiyonlar icra eden kartlar	0	69	0.0	100.0
• Fotoğraflı kimlik kartları	17	52	24.6	75.4
• Optik kodlu kimlik kartları	3	66	4.3	95.7
• Elektrik kodlu kimlik kartları	1	68	1.4	98.6
• Manyetik kodlu kimlik kartları	13	56	18.8	81.2
• Akıllı kartlar	0	69	0.0	100.0
• Hiçbiri	34	35	49.3	50.7
• Diğer. (Belirtiniz)	0	69	0.0	100.0

EK-1. *Anket Soruları Değerlendirme Sonuçları (devam)*

12.Bilgisayar sisteminizin yerleşik olduğu mevki nedir?	*Frekans*	*Nisbi Frekans(%)*
• Bodrum	9	13.0
• Zemin Kat	16	23.2
• Üst Katlar	42	60.9
• Diğer (Belirtiniz)	2	2.9
13. Bilgisayar sisteminizin bulunduğu yere kaç adet giriş/çıkış mevcuttur?		
• Bir	49	71.0
• İki	16	23.2
• İkiden Fazla	4	5.8

Sorular ve Seçenekler	*Frekanslar*		*Nisbi Frekanslar(%)*	
	Evet	*Hayır*	*Evet*	*Hayır*
14. Sisteminizde kullandığınız uygulama programlarında kasti olarak yapılan herhangi bir sahtekarlık tespit ettiniz mi?	1	68	1.4	98.6
15. Yukarıdaki soruya cevabınız "evet" ise cinsini belirtiniz.				
16. Bilgisayar işlemlerinin istendiği şekilde yürütülmesi için aşağıdaki prosedürlerin hangileri uygulanmaktadır?				
• Veri kullanım sorumluluğunun verileri işleyen kullanıcılara verilmesi	36	33	52.2	47.8
• Bilgisayar sisteminin faaliyetlerine ilişkin kayıtların tutulması	37	32	53.6	46.4
• Çıktıların kuryeler tarafından dağıtıldığı durumlarda kuryelerin güvenilirliğinin test edilmesi	5	64	7.2	92.8
• Verilerin hassasiyet seviyesine göre sınıflandırılması	18	51	26.1	73.9
• İşe yaramayan ya da artık kullanılmayan dokümanların tahrip edilmesi	30	39	43.5	56.5
• Güvenlik raporlarının gizliliğinin sağlanması	20	49	29.0	71.0
• Manyetik disk ve teyplerin etiketlenmesi	69	0	100.0	0.0
• Hassas dokümanlar ve bilgisayar donanımı üzerine koyulmuş ikazlar	12	57	17.4	82.6
• Çalışanların sorumluluklarını ayrıntılı bir şekilde açıklayan yazılı politika ve prosedürler	26	43	37.7	62.3
• Verileri kullananlarla değişiklik yapma yetkisi olanların ayrılması	54	15	78.3	21.7
• Manyetik teyp seri no, raf vb. bilgi veri tabanının bulundurulması	23	46	33.3	66.7

EK 1: *Anket Soruları Değerlendirme Sonuçları (devam)*

Sorular ve Seçenekler	Frekanslar		Nispi Frekansları(%)	
	Evet	Hayır	Evet	Hayır
• Manyetik teyplerin organizasyon dışında güvenilir yerlerde muhafaza edilmesi	41	28	59.4	40.6
• Diğer.(Belirtiniz)	2	67	2.9	97.1
17.Personel hakkında aşağıdaki kontrollerden hangilerini uyguluyorsunuz?				
• Yeni personel alımlarında referansların ve kişisel bazı bilgilerin kontrol edilmesi	50	19	72.5	27.5
• Personelin organizasyondan ayrıldıktan sonra firma sırlarını ifşa etmemesi konusunda imzalı beyannameler alınması	7	62	10.1	89.9
• Suiistimalleri önlemek amacıyla personelin değişik zamanlarda rotasyona tabi tutularak değişik yerlerde çalıştırılması	4	65	5.8	94.2
• İşten ayrılanların sistemdeki hesaplarının derhal iptali veya şifrelerinin değiştirilmesi	49	20	71.0	29.0
• İşten ayrılanların son zamanlarda yaptıkları faaliyetlerin izlenmesi	11	58	15.9	84.1
• Personel hakkındaki özel bilgileri ihtiva eden dosyalara direk erişimin engellenmesi	44	25	63.8	36.2
• Hiçbiri	3	66	4.3	95.7
• Diğer.(Belirtiniz)	0	69	0.0	100.0
18. Bilgisayar güvenliği ile ilgili olarak personel için eğitim programlarınız var mıdır?	20	49	29.0	71.0
19. Yukarıdaki soruya cevabınız "evet" ise bu eğitimde hangi yollar kullanılıyor?				
• Bilgisayarların ve sistemin güvenliği konusunda personelin rolleri anlatılıyor.	15	5	75.0	25.0
• Bilgisayar ve sistem güvenlik politika ve prosedürlerinin nasıl uygulanacağı öğretiliyor.	9	11	45.0	55.0
• Şirket yayınlarında güvenlik konusunda makaleler yayınlanıyor.	2	18	10.0	90.0
• Departman şefleri ve diğer idareciler için güvenlik tezkereleri hazırlanıyor.	4	16	20.0	80.0
• Bilgisayar güvenliği konusunda uzmanlar tarafından yayınlanmış makalelerden faydalanılıyor.	4	16	20.0	80.0
• Güvenlik alanında uzman kişiler getirilerek seminerler düzenleniyor.	5	15	25.0	75.0
• Diğer.(Belirtiniz)	0	20	0.0	100.0

EK 1: *Anket Soruları Değerlendirme Sonuçları (devam)*

Sorular ve Seçenekler	Frekanslar		Nisbi Frekanslar (%)	
	Evet	Hayır	Evet	Hayır
20. Aşağıdaki teknik güvenlik tedbirlerinden sisteminizde uygulananları işaretleyiniz.				
• Belli terminallerin belli işlemleri yapmak için yetkili olduklarını ayırmaz amacıyla terminal tanımlayıcı devrelerin kullanılması	30	39	43.5	56.5
• Bilgisayar programında yapılan değişiklikleri izleme raporları	28	41	40.6	59.4
• Satın alınan yazılım ve donanım için satıcı firmalardan tamir ve bakım garantisinin alınması	61	8	88.4	11.6
• Hassas verilerin enkript edilerek (şifreleyerek) tanınmaz hale getirilmesi	9	60	13.0	87.0
• Terminal erişimlerinde şifrelerin kullanılması	69	0	100.0	0.0
• Veri dosyalarına erişimin kontrolü	47	22	68.1	31.9
• Veri ve programların yedeklenmesi	64	5	92.8	7.2
• Şifre dosyasının enkripsiyonu	30	39	43.5	56.5
• Kullanıcı haklarının tayin ve kontrolü	59	10	85.5	14.5
• Bilgisayar kullanımının izlenmesi	46	23	66.7	33.3
• Diğer (Belirtiniz)	0	69	0.0	100.0
21. Sisteme erişim modemler vasıtasıyla mümkün müdür?	56	13	81.2	18.8
22. Yukarıdaki soruya cevabınız "evet" ise sisteminizde kullandığınız modemler call-back modemler midir?	31	25	55.4	44.6
23.Şifreleri nasıl oluşturuyorsunuz?				
• Kullanıcıların istediği şifreleri veriyoruz	31	38	44.9	55.1
• Şifreleri bilgisayarla tesadüfi olarak üretiyoruz	2	67	2.9	97.1
• Sistem yöneticisi yada sistem güvenlik görevlisi tarafından veriliyor	47	22	68.1	31.9
24. Hassas şifreleri ne kadar sıklıkla değiştiriyorsunuz?				
• Ayda bir	21	48	30.4	69.6
• Altı ayda bir	3	66	4.3	95.7
• Yılda bir	2	67	2.9	97.1
• Süre sözkonusu değil	36	33	52.2	47.8
• Diğer (Belirtiniz)	7	62	10.1	89.9
25. Sisteme login yapma esnasında hangi sınırlamalarınız mevcuttur?				
• Belli sayıda başarısız login denemesinden sonra sistemin belli bir süre login yapma izni vermemesi	35	34	50.7	49.3

EK 1:. *Anket Soruları Değerlendirme Sonuçları (devam)*

Sorular ve Seçenekler	Frekanslar		Nisbi Frekanslar (%)	
	Evet	Hayır	Evet	Hayır
• Belli sayıda başarısız login denemesinden sonra sistemin hesabı kilitlemesi	3	66	4.3	95.7
• Şifreye ilaveten bir kişisel tanıtım numarası ya da bir proje numarası	18	51	26.1	73.9
• Login yapma için bir müddet koyulması (örneğin 30 sn.)	13	56	18.8	81.2
• Belli bir süre içerisinde belli sayıda başarısız login denemesinden (örneğin yılda 500 adet) sonra hesabın tamamen kilitlenmesi	13	56	18.8	81.2
• Belli bir süre sonunda belli bir sayıda başarısız login denemesinden sonra (örneğin 100 adet) şifrenin, müddeti sona ermiş şifre olarak işlem görüp değiştirilmesinin mecbur edilmesi	6	63	8.7	91.3
• Herhangi bir sınırlama yok	19	50	27.5	72.5
• Diğer (Belirtiniz)	0	69	0.0	100.0
26. Şifrelerin yapısı konusunda kullanıcıları mecbur tuttuğunuz ya da sistem tarafından getirilen sınırlamalarınız nelerdir?				
• Şifreler en az 6 karakter uzunluğunda olmalıdır	36	33	52.2	47.8
• Şifrelerin içlerinde özel karakterler bulunması mecburiyeti	10	59	14.5	85.5
• Kişisel bilgilerin (ad, soyad, tel. no, plaka no vb) herhangi bir şeklinin (tersten, büyük harf, karışım şeklinde) şifre olarak kullanılmaması mecburiyeti	13	56	18.8	81.2
• Herhangi bir sınırlama yok	28	41	40.6	59.4
• Diğer (Belirtiniz)	4	65	5.8	94.2
27. Şifrelerin değiştirilmesi istendiği veya gerektiği durumlarda kim tarafından değiştiriliyor?				
• Kullanıcılar tarafından değişimi mümkün kılan mekanizmalar mevcut	44	25	63.8	36.2
• Sistem yöneticisi ya da sistem güvenlik görevlisi tarafından değiştiriliyor	25	44	36.2	63.8
28. Eğer PC tabanlı sistemler ya da stand-alone PC'ler kullanılıyorsa virüs ve benzeri kötü niyetli yazılımlardan etkilendiniz mi?	32	37	46.4	53.6
• 29. Yukarıdaki soruya cevabınız "evet" ise sistemin enfekte edildiğini nasıl keşfettiniz?				
• Ekranda garip mesajlar belirdi	13	19	40.6	59.4
• Veriler ve programlar silindi	17	15	53.1	46.9
• Sistem kilitlendi	27	5	84.4	15.6

EK-1. Anket Soruları Değerlendirme Sonuçları (devam)

Sorular ve Seçenekler	Frekanslar		Nisbi Frekanslar(%)	
	Evet	Hayır	Evet	Hayır
• Sistemde gariplikler başladı	8	24	25.0	75.0
• Anti-virüs yazılımlarıyla sistemi tararken	16	16	50.0	50.0
• Diğer.(Belirtiniz)	2	30	6.2	93.8
30. Sisteminizi ne tür virüsler etkiledi?				
• Boot sektör virüsleri	25	44	36.2	63.8
• İşletim sistemini etkileyen virüsler	15	54	21.7	78.3
• Uygulama programlarını ve veri dosyalarını etkileyen virüsler	22	47	31.9	68.1
31. Virüslere karşı ne gibi koruma tedbirleriniz mevcuttur?				
• Anti-virüs yazılımları kullanıyoruz	48	21	69.6	30.4
• Çeşitli seminer ve toplantılarla kullanıcıları eğitiyoruz	13	56	18.8	81.2
• Yazılımları ve verileri yedekliyoruz	34	35	49.3	50.7
• Disketleri daha önce kontrolden geçirip sonra kullanıyoruz	34	35	49.3	50.7
• Sistemimizde kesinlikle lisanssız kopya programları kullanmıyoruz	20	49	29.0	71.0
• İllegal erişimleri kontrol eden sistem izleme araçları kullanıyoruz	4	65	5.8	94.2
• Programların hacim, tarih ve muhteva olarak değişip değişmediğini kontrol eden yazılımlar kullanıyoruz	3	66	4.3	95.7
• Özel bir tedbir almıyoruz	18	51	26.1	73.9
• Diğer.(Belirtiniz)	1	68	1.4	98.6