

**Gamze DÜZENLİ**

**120757031**

**BMS-302 Bilgisayar-Bilgi Güvenliği ve Yönetimi**

**Prof.Dr. Abdulsamet HAŞILOĞLU**

**İÇİNDEKİLER**

**GİRİŞ……………………………………………………………………………………………………1**

**BİLGİ GÜVENLİĞİ KONTROL TÜRLERİ………………………………………………………...1**

**FİZİKSEL KONTROLLER…………………………………………………………………………...1**

**Önleyici Fiziksel Kontroller…………………………………………………………………………....2**

**Dedektif Fiziksel Kontroller……………………………………………………………………………3**

**TEKNİK KONTROLLER……………………………………………………………………………..4**

**Önleyici Teknik Kontroller………………………………………………………………………….....4**

**Dedektif Teknik Kontroller…………………………………………………………………………….5**

**İDARİ KONTROLLER………………………………………………………………………………..5**

**Önleyici İdari Kontroller………………………………………………………………………………5**

**Dedektif İdari Kontroller………………………………………………………………………………7**

**TEKNOLOJİ VE GİZLİLİK ÇATIŞTIĞINDA……………………………………………………..9**

**Şifreleme ve Gizli Mesajlar…………………………………………………………………………….9**

**Mevcut Mevzuat………………………………………………………………………………………...10**

**Gizlilik Hakları………………………………………………………………………………………….10**

**Veri Şifreleme Standardı……………………………………………………………………………….11**

**Clipper Tartışması………………………………………………………………………………………11**

**EAVESDROPPİNG NEDİR?..................................................................................................................12**

**Aktif Eavesdropping Saldırısı…………………………………………………………………………..12**

**Pasif Eavesdropping Saldırısı…………………………………………………………………………...13**

**Wireshark ile Pasif Eavesdropping……………………………………………………………………..13**

**Eavesdropping Saldırılarından Nasıl Korunulmalıdır?.........................................................................13**

**KAYNAKLAR……………………………………………………………………………………………14**

**GİRİŞ**

Erişim Kontrolü Yönetimi bölümü olan 1.2 bölümünün Bilgi Güvenliği Kontrol Türleri ve Teknoloji ve Gizlilik Çatıştıdığında konuları olan ve bunlara ek olarak Gizli Dinleme (Eavesdropping) konusunu anlatacağım.

**BÖLÜM 1.2 ERİŞİM KONTROLÜ YÖNETİMİ**

**BİLGİ GÜVENLİĞİ KONTROL TÜRLERİ**

*Harold F. Tipton*

Güvenlik genellikle tehlikeden arınma veya emniyet koşulu olarak tanımlanır. Özellikle bilgisayar güvenliği, bir sistemdeki verilerin yetkisiz ifşa edilmesine, değiştirilmesine veya bilgisayar sisteminin kendisinin yetkisiz kullanıma, değiştirilmesine veya hizmet reddine karşı korunmasına karşı korunmasıdır. Bazı bilgisayar güvenlik kontrolleri üretkenliği engellediğinden, güvenlik tipik olarak güvenlik uygulayıcılarının, sistem kullanıcılarının ve sistem operasyonlarının ve idari personelin güvenlik ve verimlilik arasında tatmin edici bir denge sağlamak için çalıştığı bir uzlaşmadır.

Bu üç kontrol kategorisi ayrıca önleyici veya dedektif olarak sınıflandırılabilir. Önleyici kontroller istenmeyen olayların ortaya çıkmasını önlemeye çalışmakta, dedektif kontroller ise meydana geldikten sonra istenmeyen olayları tanımlamaya çalışmaktadır. Önleyici kontroller, bilgisayar kaynaklarının serbest kullanımını engeller ve bu nedenle yalnızca kullanıcıların kabul etmeye istekli olduğu dereceye uygulanabilir. Etkili güvenlik bilinci programları, kullanıcıların bu tür denetimlerin bilgisayar sistemlerine güvenmelerini nasıl sağladığını anlamalarına yardımcı olarak önleyici denetimlere karşı tolerans düzeyini artırmaya yardımcı olabilir. Yaygın dedektif denetimleri denetim izlerini, izinsiz giriş tespit yöntemlerini ve sağlama toplamlarını içerir.

Diğer üç kontrol türü önleyici ve dedektif kontrolleri destekler. Genellikle caydırıcı, düzeltici ve kurtarma olarak tanımlanırlar. Caydırıcı kontroller, bireyleri bilişim güvenliği politikalarını veya prosedürlerini kasıtlı olarak ihlal etmekten caydırmak için tasarlanmıştır. Bunlar genellikle yetkisiz faaliyetleri veya sonuçların tehditlerini, güvenlik ihlalini engellemeyecek potansiyel bir davetsiz misafirin (örneğin utançtan ağır cezalara kadar değişen tehditler gibi) gerçekleştirmesini zorlaştırır veya istemez kılan kısıtlamalar biçimini alır.

Düzeltici kontroller ya izinsiz faaliyete izin veren koşulları giderir ya da ihlallerden önce oldukları koşullara geri döner. Düzeltici kontrollerin uygulanması, mevcut fiziksel, teknik ve idari kontrollerde değişikliklere neden olabilir. Kurtarma denetimleri, kayıp bilgi işlem kaynaklarını veya yeteneklerini geri yükler ve kuruluşun güvenlik ihlallerinden kaynaklanan parasal kayıpları kurtarmasına yardımcı olur.

Caydırıcı, düzeltici ve geri kazanım kontrolleri, fiziksel, teknik ve idari kontrollerin ana kategorileri içerisinde özel durumlar olarak kabul edilir; açıkça önleyici veya dedektif kategorilerine girmiyorlar. Örneğin, caydırıcılığın bir önleyici biçimi olduğu söylenebilir, çünkü bir davetsiz misafirin geri dönmesine neden olabilir; ancak caydırıcılık aynı zamanda davetsiz misafirin en çok korktuğu şey olan ihlalleri tespit etmeyi de içerir. Öte yandan, düzeltici kontroller önleyici ya da dedektif değildir, ancak antiviral yazılım bir virüsü yok ettiğinde teknik kontrollerle veya yedekleme prosedürleri zarar görmüş bir veri tabanını geri yüklemeyi sağladığında idari kontrollerle açıkça bağlantılıdır. Son olarak, kurtarma kontrolleri ne önleyici ne de dedektif değildir, ancak felaket kurtarma veya acil durum planları olarak idari kontrollere dahil edilir.

Fiziksel, teknik ve idari kontrollerle olan bu çakışmalardan dolayı caydırıcı, düzeltici ve kurtarma kontrolleri bu bölümde daha fazla ele alınmamaktadır. Bunun yerine, üç ana kategorideki önleyici ve dedektif kontroller incelenmiştir.

**FİZİKSEL KONTROLLER**

Fiziksel güvenlik, bilgisayarlara, ilgili ekipmanlara (tesisler dahil) ve işleme tesisinin kendisine erişimi kontrol etmek için kilitlerin, güvenlik görevlilerinin, rozetlerin, alarmların ve benzeri önlemlerin kullanılmasıdır. Ek olarak, bilgisayarların, ilgili ekipmanların ve bunların içeriklerinin casusluk, hırsızlık ve imha veya kaza, yangın veya doğal afet (örneğin, ani ve depremler) kaynaklı hasarlardan korunma önlemleri alınmalıdır.

**Önleyici Fiziksel Kontroller**

Yetkili olmayan personelin bilgi işlem olanaklarına girmesini engellemek (yani bilgisayar kaynaklarını barındıran yerler, yardımcı programları, bilgisayar basılı kopyalarını ve girdi veri ortamlarını) önlemek ve doğal afetlere karşı korunmaya yardımcı olmak için önleyici fiziksel kontroller kullanılır. Bu kontrollerin örnekleri arasında şunlar bulunur:

* Yedek dosyalar ve belgeler.
* Parmaklıklar.
* Güvenlik görevlileri.
* Rozet sistemleri
* Çift kapı sistemleri.
* Kilitler ve anahtarlar.
* Yedek güç.
* Biyometrik erişim kontrolleri.
* Yer seçimi.
* İtfaiyeciler.

**Yedekleme Dosyaları ve Belgeler:** Bir kaza veya davetsiz misafir aktif verileri veya belgeleri yok ederse, yedek kopyaların hazır bulunması önemlidir.Orijinalleri tahrip eden aynı olayın imhasını önlemek için yedekleme dosyaları aktif veri veya dokümantasyondan yeterince uzakta saklanmalıdır.Yedek malzeme, iki saatlik duvarlar dahil, yanmaz malzemelerden yapılmış güvenli bir yerde muhafaza edilmelidir.Hassas bilgilerin yedekleri, bu bilgilerin aktifleriyle aynı koruma seviyesine sahip olmalıdır; sistemdeki veriler için sıkı bir güvenlik sağlamak anlamsızdır, ancak aynı veriler için yedek bir yerde gevşek güvenlik sağlar.

**Parmaklıklar:** Her ne kadar binanın etrafındaki çitler, belirli bir davetsiz misafire karşı çok fazla koruma sağlamamasına rağmen, resmi izinsiz giriş hattı kurarlar ve basitçe meraklı kişiyi caydırabilirler. Çitler alarm vermeli veya korumalar, köpekler veya TV monitörleri tarafından sürekli gözetim altında tutulmalıdır.

**Güvenlik Görevlileri:** Güvenlik görevlileri, davetsiz misafirleri engellemek ve yalnızca yetkili kişilerin girmesine izin verildiğinden emin olmak için çoğu kez tesislerin girişlerine yerleştirilir. Gardiyanlar, yalnızca yetkili, doğru şekilde tanımlanmış eşyaların tesise girip çıkmalarını sağlamak için paketlerin veya elden taşınan diğer eşyaların incelenmesinde etkilidir. Bina, güvenlik istasyonunda sonlanan alarmlar veya diğer uyarı göstergeli uygun elektronik dedektörlerle kablolandığında, sabit korumaların etkinliği büyük ölçüde artırılabilir. Ek olarak, gardiyanlar, izinsiz girişlerden izinsiz giriş yapmalarını engellemek için normal çalışma saatlerinden sonra binaların içindeki gözetimsiz alanları devriye gezmek için kullanılır.

**Rozet Sistemleri:** Bilgi işlem alanlarına fiziksel erişim, bir rozet sistemi kullanılarak etkin bir şekilde kontrol edilebilir. Bu kontrol yöntemiyle çalışanlar ve ziyaretçiler erişim kontrolündeki her alanda uygun rozetleri giymelidir. Sadece yetkili kişilerin girişine izin vermek için programlanan rozet okuma sistemleri davetsiz misafirleri kolayca tespit edebilir.

**Çift Kapı Sistemleri:** Çift kapı sistemleri, insanları güvenli bölgeye bırakılmadan önce kendilerini korumaya tanıtmaya zorlamak için sınırlı alanlara (örneğin bilgisayar olanakları) girişlerde kullanılabilir. Çift kapılar, davetsiz misafirlerin izin verilen kişilerin arkasını takip etmelerini ve kısıtlı alanlara kaymalarını engellemenin mükemmel bir yoludur.

**Kilitler ve Anahtarlar:** Kilitler ve anahtarlar, sınırlı alanlara erişimi kontrol etmek için yaygın olarak kullanılır. Anahtarların kopyalanmasını kontrol etmek zor olduğundan, çoğu kurulum şifre kilitleri kullanır (yani, uygun sırayla basıldığında kilidi açan düğmeler içeren şifreli kilitler) kullanır. Şifre kilitleri ile, kombinasyondan ödün vermemek için hangi düğmelere basıldığına dikkat edilmelidir.

**Yedek Güç:** Bilgisayar hizmetlerinin sürekli hazır olma durumunda olmalarını sağlamak ve normal güç kaybı durumunda ekipmana zarar gelmesini önlemek için yedek güç gerekir. Kısa süreli güç kaybı için, yedek güç genellikle piller tarafından sağlanır. 15-30 dakikadan daha uzun süren kesintilere duyarlı alanlarda genellikle dizel jeneratörler önerilir.

**Biyometrik Geçiş Kontrolleri:** Biyometrik tanımlama, bilgisayar tesislerine erişimi kontrol etmede rozet okuyuculardan daha karmaşık bir yöntemdir, ancak iki yöntem de aynı şekilde çalışır. Tanımlama için kullanılan biyometri, gerngerprints, handprints, ses düzenleri, imza örnekleri ve retina taramalarını içerir. Biyometri kaybedilme, çalınma veya paylaşılamadığından, rozetlerden daha yüksek bir güvenlik seviyesi sağlarlar. Yüksek güvenlikli, düşük trafikli giriş kontrolü için biyometrik tanımlama önerilir.

**Yer Seçimi:** Bilgi işlem olanaklarına ev sahipliği yapan binanın bulunduğu alan, belirgin risklerden kaçınmak için dikkatlice seçilmelidir. Örneğin, ormanlık alanlar tehlike yaratabilir, bir deprem hatasının bitişiğindeki veya yanındaki alanlar tehlikeli olabilir ve bir ovada bulunan alanlar su hasarına karşı hassastır. Ek olarak, bir uçak yaklaşımı ya da kalkış rotası altındaki konumlar risklidir ve demiryolu raylarına bitişik konumlar ekipman sorunlarını çökertebilecek titreşimlere karşı hassas olabilir.

**İtfaiyeciler:** Acil durumun kontrolü, acil durumun veri işlemeyi ciddi şekilde engelleyen bir felakete dönüşmesini önlemek için önemlidir. Bilgi işlem olanakları potansiyel kaynaklardan uzakta (örneğin mutfak veya kafeterya) bulunmalı ve yanıcı olmayan malzemelerden yapılmalıdır. Mobilyalar da yanmaz nitelikte olmalıdır. Kolay erişim için uygun yangın söndürücü tiplerinin uygun bir şekilde yerleştirilmesi önemlidir. Çalışanlar yangın söndürücülerinin uygun kullanımı ve patlak vermesi gereken prosedürler konusunda eğitilmelidir.

Otomatik fıskiyeler bilgisayar odaları ve çevresindeki alanlarda ve yüksek zeminlerde pahalı ekipmanlar bulunduğunda çok önemlidir. Sprinkler, yanıcı malzemeler içeren herhangi bir bilgisayar odasının korunması için genellikle sigorta şirketleri tarafından belirlenir. Bununla birlikte, bilgisayar ekipmanında su hasarı riski genellikle damage hasar riskinden daha fazladır. Bu nedenle, karbon dioksit söndürme sistemleri geliştirilmiştir; bu sistemler, havadaki oksijeni gidererek baskı altına alan karbondioksit ile tehdit edilen bir bölgeye sahiptir. Her ne kadar karbondioksit suya zarar vermese de, bölgedeki insanlar için potansiyel olarak öldürücüdür ve şimdi yalnızca gözetimsiz alanlarda kullanılmaktadır.

Mevcut yangın söndürme sistemleri, genellikle donanıma zarar vermeyen ve personel için karbondioksitten daha az tehlikeli olan Halon bölgesini aşmıştır. Yaklaşık% 10'luk bir konsantrasyonda, Halon yangın söndürür ve insanlar tarafından güvenli bir şekilde nefes alabilir. Bununla birlikte, daha yüksek konsantrasyonlar sonunda bir sağlık tehlikesi oluşturabilir. Ek olarak, Halon'u basınç altında serbest bırakmaktan kaynaklanan patlama, etraftaki gevşek nesneleri uçurabilir ve ekipman ve personel için tehlike oluşturabilir. Bu nedenlerden dolayı ve Halon'un yüksek maliyeti nedeniyle, genellikle bilgisayar odalarında yalnızca yüksek zeminlerde kullanılır. Kloro-ürokarbonlar içerdiğinden, yakında çevreye daha az zararlı olan bir gaz lehine geçecektir.

**Dedektif Fiziksel Kontroller**

Dedektif fiziksel kontroller, koruyucu hizmetler personelini, fiziksel güvenlik önlemlerinin ihlal edildiği konusunda uyarmaktadır. Bu kontrollerin örnekleri arasında şunlar bulunur:

* Hareket detektörleri.
* Duman ve alev dedektörleri.
* Kapalı devre televizyon monitörleri.
* Sensörler ve alarmlar.

**Hareket Dedektörleri:** Genellikle içinde insan olmayan bilgisayar tesislerinde, hareket dedektörleri potansiyel izinsiz girişlere dikkat çekmek için kullanışlıdır. Hareket dedektörleri, korumalar tarafından sürekli izlenmelidir.

**Yangın ve Duman Dedektörleri:** Yangın ve duman dedektörleri bir yangının erken uyarısını sağlamak için stratejik olarak yerleştirilmelidir. Tüm tespit ekipmanı çalışır durumda olduğundan emin olmak için periyodik olarak test edilmelidir.

**Kapalı Devre Televizyon Monitörleri:** Kapalı devre televizyonlar, kullanıcıların veya operatörlerin sık sık bulunmadığı bilgi işlem alanlarındaki faaliyetleri izlemek için kullanılabilir. Bu yöntem, bireylerin şüpheli davrandıklarını tespit etmeye yardımcı olur.

**Sensörler ve Alarmlar:** Sensörler ve alarmlar, hava ve soğutma suyu sıcaklıklarının ekipman tasarımı tarafından belirtilen seviyelerde kalmasını sağlamak için ekipmanı çevreleyen ortamı izler. Uygun koşullar sağlanmazsa, alarmlar bir iş kesintisi oluşmadan önce durumu düzeltmek için operasyonları ve bakım personelini çağırır.

**TEKNİK KONTROLLER**

Teknik güvenlik, bilgisayar donanımı, işlemler veya uygulama yazılımları, iletişim donanımı ve yazılımı ile ilgili cihazlarda bulunan güvenlik önlemlerinin kullanılmasını içerir. Teknik kontrollere bazen mantıksal kontroller denir.

**Önleyici Teknik Kontroller**

Önleyici teknik kontroller, yetkisiz personel veya programların bilgi işlem kaynaklarına uzaktan erişimini engellemek için kullanılır. Bu kontrollerin örnekleri arasında şunlar bulunur:

* Erişim kontrolü yazılımı.
* Antivirüs yazılımı.
* Kütüphane kontrol sistemleri.
* Şifreler.
* Akıllı kartlar.
* Şifreleme.
* Çevirmeli erişim kontrolü ve geri arama sistemleri.

**Erişim Kontrol Yazılımı:** Geçiş kontrol yazılımının amacı, kullanıcılar arasında veri ve programların paylaşımını kontrol etmektir. Birçok bilgisayar sisteminde, verilere ve programlara erişim, hangi kullanıcıların erişime izin verildiğini belirleyen erişim kontrol listeleri tarafından uygulanır. Erişim kontrolü yazılımı, yalnızca yetkili oturum açma kimliği ve şifresi olan kayıtlı kullanıcıların bilgisayar sistemine erişim kazanabileceğini belirleyerek sisteme erişimi denetleme olanağı sağlar.

Sisteme erişim verildikten sonra, bir sonraki adım sistemde bulunan verilere ve programlara erişimi kontrol etmektir. Veri veya program sahibi, verileri veya programı kullanma yetkisi olan kişileri belirleyebilir.

**Antivirüs Yazılımı:** Virüsler, mikro bilgi işlem dünyasında salgın oranlara ulaşmış ve işlem yapılırken işlem bozulmalarına ve veri kaybına ve ayrıca temizlik sırasında önemli verimlilik kaybına neden olabilir. Buna ek olarak, sürekli artan bir oranda yeni virüsler ortaya çıkıyor - şu anda yaklaşık her 48 saatte bir. Virüsleri algılamak, tanımlamak, izole etmek ve ortadan kaldırmak için virüsten koruma yazılımının tüm mikro bilgisayarlara yüklenmesi önerilir. Yeni virüslere yardımcı olmak için bu yazılım sık sık güncellenmelidir. Ek olarak, virüslerin mümkün olduğunca erken ele geçirilmesine yardımcı olmak için, virüsten koruma yazılımı, kullanıcıların takdirine bağlı olarak aralıklı olarak kullanılmayan bir sistemde etkin tutulmalıdır.

**Kütüphane Kontrol Sistemleri:** Bu sistemler, üretim programlarındaki tüm değişikliklerin, değişiklikleri oluşturan programcılar yerine kütüphane kontrol personeli tarafından yapılmasını gerektirir. Bu uygulama, üretim programlarında yetkisiz değişiklik yapılmasını önleyen görevlerin ayrılmasını sağlar.

**Şifreler:** Parolalar, bir kimliğin kullanıcısının kimliğin sahibi olduğunu doğrulamak için kullanılır. Kimlik şifresi kombinasyonu, her kullanıcı için benzersizdir ve bu nedenle, kullanıcıların sistemdeki etkinliklerinden sorumlu olmalarını sağlar.

Belirli bir süre için kullanılan sabit şifreler, bilgisayar korsanlarının ödün vermesi için genellikle kolaydır; bu nedenle, bu şifrelerin herhangi bir sözlükte görünmemesi için büyük özen gösterilmelidir. Sabit şifreler genellikle belirli veri tabanlarına erişimi kontrol etmek için kullanılır. Bununla birlikte, bu kullanımda, veri tabanına erişim yetkisi olan herkes aynı şifreyi kullanır; bu nedenle sorumluluk alınamaz.

Günümüzde, her oturum açma için farklı olan dinamik veya bir defalık şifreler şifreli şifrelere göre tercih edilmektedir. Dinamik şifreler, rasgele şifreler oluşturmak için programlanmış bir belirteç tarafından oluşturulur.

**Akıllı Kartlar:** Akıllı kartlar genellikle bir kredi kartının boyutuyla ilgilidir ve belirli bir kullanıcının ayrıcalıklarını tanımlamak için uzak bir terminalde okunabilen mantık fonksiyonları ve bilgileri olan bir çip içerir. Akıllı kartlar artık, bilgisayara veya ağa erişim yetkisini doğrulamak için kullanıcının sağladığı verilerle (örneğin kişisel bir kimlik numarası veya biyometrik veriler) karşılaştırılan önceden kaydedilmiş, genellikle şifreli erişim denetimi bilgilerini taşır.

**Şifreleme:** Şifreleme, düz metinlerin (yani okunabilir veriler) şifreli tekniklerle şifreli metinlere (yani okunamaz veriler) dönüşümü olarak tanımlanır. Şifreleme, verileri ağ iletimleri sırasında ifşa edilmekten korumanın tek kesin yolu olarak kabul edilmektedir.

Şifreleme donanım veya yazılım ile uygulanabilir. Yazılım tabanlı şifreleme en ucuz yöntemdir ve düşük hacimli yayınlar içeren uygulamalar için uygundur; Yazılımın büyük miktarda veri için kullanılması, işlem maliyetlerinde kabul edilemez bir artışa neden olur. Donanım şifrelemeyle ilgili hiçbir ek yük olmadığı için, büyük miktarlarda veri söz konusu olduğunda bu yöntem tercih edilir.

**Çevirmeli Erişim Kontrolü ve Geri Arama Sistemleri:** Bir bilgisayar sistemine çevirmeli erişim bilgisayar korsanları tarafından izinsiz girme riskini artırır. Kişisel bilgisayarlar içeren veya diğer ağlara bağlı olan şebekelerde, çevirmeli ağ bağlantısının çevirmeli hale getirilmesi için kişisel bir bilgisayara modem eklenebilme kolaylığı nedeniyle çevirmeli erişimin uygun olup olmadığını belirlemek zordur. erişim noktası. Bilinen çevirmeli bağlantı noktalarının yalnızca yetkili çevirmeli bağlantı kullanıcılarının erişebilmesi için kontrol edilmesi gerekir.

Şu anda, en iyi çevirmeli erişim denetimleri, çağrıları kesmek, arayan kişinin kimliğini doğrulamak (dinamik bir parola mekanizması kullanarak) ve kullanıcıyı istediğiniz şekilde yetkili bilgisayar kaynaklarına geçirmek için bir mikro bilgisayar kullanıyor. Önceden, geri arama sistemleri, arama yapanları aramaya başladı, yetkilerini doğruladı ve ilk olarak etkili olduklarını gösteren kayıtlı numaralarına geri çağırdı. Bununla birlikte, sofistike bilgisayar korsanları, çağrı yönlendirme teknikleri kullanarak bu kontrolün nasıl yenileceğini öğrendi.

**Dedektif Teknik Kontroller**

Dedektif teknik kontroller personeli ihlallere karşı uyarır veya önleyici teknik kontrollerin ihlal edilmesine teşebbüs eder. Bunlara örnek olarak, takip eden bölümlerde ele alınan denetim izleri ve izinsiz giriş tespit uzman sistemleri dahildir.

**Denetim İzleri:** Bir denetim izi, bir işlemin olay sıralamasının başlangıcından son sonuçların çıktısına kadar yeniden yapılandırılmasını ve incelenmesini sağlayan sistem faaliyetlerinin bir kaydıdır. İhlal raporları, denetim izinde öngörülen fiili veya teşebbüs politika geçişlerini gösterebilecek önemli, güvenlik odaklı olaylar sunmaktadır. İhlal raporları, başarılı veya başarısız yetkisiz erişimleri tespit etmek ve araştırmak için araştırmacılar ve veri tabanı sahiplerinin güvenliği tarafından sık sık ve düzenli olarak gözden geçirilmelidir.

**Saldırı Tespit Sistemleri:** Bu uzman sistemler kullanıcıları (kişisel performanslarına göre) takip ederken mevcut faaliyetlerinin belirlenmiş bir normla tutarlı olup olmadığını belirlemek için sistemi kullanıyorlar. Aksi takdirde, kullanıcının oturumu sonlandırılabilir veya araştırmak için bir güvenlik çağrısı yapılabilir. İzinsiz giriş tespiti, özellikle davetsiz misafirlerin yetkili kullanıcılar gibi davrandığı durumlarda veya yetkili kullanıcılar yetkisiz faaliyetlerde bulunduğunda etkili olabilir.

**İDARİ KONTROLLER**

İdari veya personel güvenliği, bilgi işlem kaynakları için kabul edilebilir bir koruma seviyesi sağlamak üzere oluşturulan yönetim kısıtlamaları, operasyonel prosedürler, hesap verebilirlik prosedürleri ve tamamlayıcı idari kontrollerden oluşur. Ek olarak, idari kontroller, bilgi işlem kaynaklarına erişimi olan tüm personelin gerekli yetkilere ve uygun güvenlik mesafelerine sahip olmasını sağlamak için oluşturulan prosedürleri içerir.

**Önleyici İdari Kontroller**

Önleyici idari kontroller, bilgisayar veri ve programlarının gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak için insanların davranışlarını kontrol etmeye yönelik personel odaklı tekniklerdir. Önleyici idari kontrollere örnekler:

* Güvenlik bilinci ve teknik eğitim.
* Görevlerinin ayrılması.
* Çalışanları işe alma ve işten çıkarma prosedürleri.
* Güvenlik politikaları ve prosedürleri.
* Nezaret.
* Olağanüstü durum kurtarma, acil durum ve acil durum planları.
* Bilgisayar erişimi için kullanıcı kaydı.

**Güvenlik Bilinci ve Teknik Eğitim:** Güvenlik bilinci eğitimi, kullanıcıların güvenlik uygulamalarının faydalarını anlamalarına yardımcı olan önleyici bir önlemdir. Çalışanlar, uygulanan kontrollerin gerekliliğini anlamazlarsa, sonunda onları aşabilir ve böylece güvenlik programını zayıflatabilir veya etkisiz hale getirebilir.

Teknik eğitim, kullanıcıların en sık karşılaşılan güvenlik sorununu (hatalar ve eksiklikler) önlemesinin yanı sıra, uygun yedekleme yöntemlerini nasıl oluşturacaklarını ve virüsleri nasıl tespit edip kontrol edebileceklerini anlamalarına yardımcı olabilir. Acil servis ve işletme personeli için tatbikat şeklinde teknik eğitim, bu tür olayların afetlere tırmanmasını önlemek için uygun önlemlerin alınmasını sağlayabilir.

**Görevlerinin Ayrılması:** Bu idari kontrol, bir işlemi farklı parçalardan sorumlu farklı kullanıcılarla birlikte bir işlemi bileşen parçalara ayırır. Görevlerin adaletli bir şekilde ayrılması, bir bireyin bütün bir sürecin kontrolünü ele geçirmesini önler ve süreci kişisel kazanım için manipüle etmek için başkalarıyla çarpışmaya zorlar.

**İşe Alma ve Fesih İşlemleri:** Uygun işe alım prosedürleri, güvenlik politikalarını ihlal etmesi muhtemel kişilerin işe alınmasını önleyebilir. Başvuranın cezai tarihini ve referanslarını kontrol etmek de dahil olmak üzere kapsamlı bir arka plan araştırması yapılmalıdır. Her ne kadar bireyleri dürüstlük ve dürüstlük için mutlaka taramasalar da, daha fazla araştırılması gereken alanları belirlemeye yardımcı olabilir.

Üç tür referans alınmalıdır: (1) istihdam, (2) karakter ve (3) kredi. İstihdam referansları, bir bireyin işi için gerekli olan görevleri yerine getirme veya gerçekleştirme yetkinliğini tahmin etmesine yardımcı olabilir. Karakter referansları, güvenilirlik, güvenilirlik ve başkalarıyla iyi geçinme becerisi gibi nitelikleri belirlemeye yardımcı olabilir. Kredi referansları, bir kişinin hab nansal alışkanlıklarını gösterebilir ve bu da bir kişinin kendi eylemlerinin sorumluluğunu üstlenme konusunda olgunluk ve isteklilik göstergesi olabilir.

Ayrıca, fesih koşullarından bağımsız olarak herhangi bir çalışan şirketten ayrıldığında belirli prosedürler izlenmelidir. İsteğe bağlı olarak feshedilmiş olan çalışanlardan, bilgi işlem kaynaklarına daha fazla erişimi önlemek için, bildirimin hemen ardından tesisinden çıkmaları istenmelidir. İşçinin kararına bağlı olarak, çalışanın süreçlerini tamamlayabilmesi veya yerine geçebileceği bir eğitimi eğitebilmesi için gönüllü fesihleri ​​farklı şekilde ele alınabilir.

Bir çalışana verilen tüm yetkiler, ayrılışta iptal edilmelidir. Ayrılan çalışanın başkalarına yetki verme yetkisi varsa, bu diğer yetkiler de gözden geçirilmelidir. Binaya, bilgiye veya donanıma erişmek için kullanılan tüm anahtarlar, rozetler ve diğer cihazlar, ayrılan çalışandan alınmalıdır. Ayrılan bir çalışan tarafından bilinen tüm kilitlerin kombinasyonları derhal değiştirilmelidir. Ayrıca, çalışanın oturum açma kimlikleri ve şifreleri iptal edilmeli ve ilgili aktif ve yedek dosyalar silinmeli ya da yeni bir çalışana atanmalıdır.

Fesihle ilgili herhangi bir özel koşul (örneğin, belirli bilgilerin kullanım hakkının reddedilmesi), ayrılan çalışanla birlikte gözden geçirilmelidir. Ek olarak, bu koşulları belirten bir belge çalışan tarafından imzalanmalıdır. Tüm sonlandırmalar, sonlandırılan çalışanın tüm bilgi sistemi erişim yetkisinin iptal edilmesini sağlamak için çalıştığı tesis için bilgisayar güvenlik temsilcisi aracılığıyla yönlendirilmelidir.

**Güvenlik Politikaları ve Prosedürleri:** Uygun politika ve prosedürler, etkili bir bilgi güvenliği programının oluşturulması için kilit öneme sahiptir. Politikalar ve prosedürler, bilgilerin korunmasına ve bilgi işlem kaynaklarına ilişkin olarak kuruluşun genel politikalarını yansıtmalıdır. Politikalar, bilgisayar kaynaklarının kullanımını, hassas bilgilerin işaretlenmesini, bilgisayar dışındaki kaynakların tesis dışına taşınmasını, kişisel bilgisayar ekipmanlarının ve ortamının tesise girmesini, hassas atıkların elden çıkarılmasını ve bilgisayar ve veri güvenliği olay raporlamasını kapsamalıdır. Bu politikaların uygulanması, etkinlikleri için esastır.

**Nezaret:** Çoğu zaman, bir uyarı süpervizörü, çalışanın tutumunda bir değişiklik olduğunu fark eden ilk kişidir. İş tatminsizliğinin erken belirtileri veya kişisel sıkıntı, denetleyicileri çalışanı titizlikle kritik veya hassas bir pozisyondan uzaklaştırmayı düşünmelerini teşvik etmelidir.

Denetim otoriteleri, bölümlerinin sorumluluklarıyla ilgili politika ve prosedürleri iyice bilmelidirler. Denetim otoriteleri, çalışanlarının ilgili politika ve prosedürlere uymasını talep etmeli ve bu kılavuzların etkinliğini gözlemlemelidir. Politikaların ve prosedürlerin hedefleri daha etkili bir şekilde gerçekleştirilebilirse, denetleyici uygun iyileştirmeleri önermelidir. Görev dağılımı uygun bir görev ayrımının yapıldığından emin olmak, hassas pozisyonlardaki çalışanların zaman zaman tam bir işlem döngüsünden kaldırılmaması ve kritik veya hassas işlerin kalifiye personel arasında periyodik olarak döndürülmesini sağlamak için iş atamaları düzenli olarak gözden geçirilmelidir.

**Felaket Kurtarma, Acil Durum ve Acil Durum Planları:** Olağanüstü durum kurtarma planı, acil müdahale, genişletilmiş yedekleme işlemleri ve kurtarma için bir bilgisayar kurulumunun bilgi işlem kaynaklarının veya fiziksel tesislerin (ya da bu tesislere erişimin) kısmen ya da tamamen kaybedilmesi durumunda prosedürler içeren bir belgedir. Acil durum planları ile birlikte kullanılan bu planın temel amacı, bir bilgisayar kurulumunun felaketlerden kurtulabileceği, kritik uygulamaları bozulmuş bir modda işlemeye devam edebileceği ve makul bir çalışma modunda normal bir çalışma moduna dönebileceği konusunda makul güvence sağlamaktır. saati. Olağanüstü durum kurtarma planlamasının kilit bir parçası, orijinal tesisin müsait olmadığı zamanlarda alternatif bir alanda işlem yapılmasını sağlamaktır.

Acil durum ve acil durum planları, belirli tehditlere yönelik kurtarma prosedürleri oluşturur. Bu planlar küçük olayların felaketlere dönüşmesini önlemeye yardımcı olur. Örneğin, beklenmedik durum planı, hesaplama kabiliyetini nominal işleme döndürmek için gereken şartı ve yanıtı belirleyen bir dizi prosedür sağlayabilir; Bir acil durum planı, bir yangın durumunda ekipmanı kapatmak ya da bir deprem durumunda bir tesisi boşaltmak için özel bir prosedür olabilir.

**Bilgisayar Erişimi İçin Kullanıcı Kaydı:** Resmi kullanıcı kaydı, tüm kullanıcıların sistem ve hizmet erişimi için uygun şekilde yetkilendirilmesini sağlar. Ayrıca, kullanıcılara bilgi işlem kaynaklarının güvenliğine ilişkin sorumlulukları hakkında bilgi alma ve ilgili politika ve prosedürlere uyma konusunda anlaşma yapma fırsatını sunar.

**Dedektif İdari Kontroller**

Dedektif idari kontroller, güvenlik politikalarının ve prosedürlerinin ne kadar iyi yerine getirildiğini belirlemek, sahtekarlığı tespit etmek ve kabul edilemez bir güvenlik riski taşıyan kişilerin istihdam edilmesini önlemek için kullanılır. Bu kontrol türü şunları içerir:

* Güvenlik incelemeleri ve denetimler.
* Performans değerlendirmeleri
* Gerekli tatiller.
* Arkaplan incelemeleri.
* Görevlerin Rotasyonu

**Güvenlik İncelemeleri ve Denetimleri:** İncelemeler ve denetimler, politikaların ve prosedürlerin tatmin edici bir şekilde izlenmemesi durumlarını belirleyebilir. Verimliliği düzeltmede yönetim katılımı, bilgisayar güvenlik programı için kullanıcı desteği almada önemli bir faktör olabilir.

**Performans Değerlendirmeleri:** Düzenli olarak yapılan performans değerlendirmeleri, kalite performansını teşvik etmede önemli bir unsurdur. Ayrıca, yönetimin bilgi güvenliği ilkelerini desteklemesini güçlendirmek için etkili bir forum olabilirler.

**Zorunlu Tatiller:** Gergin çalışanların görevlerini yerine getirirken kaza yapma veya hata yapma ve ihmal etme olasılığı daha yüksektir. Tatiller, çalışanların sağlığına, genellikle uzun süreli çalışmalardan kaynaklanan gerginlik ve kaygıları hafifleterek katkıda bulunur. Buna ek olarak, kritik veya hassas pozisyonlardaki tüm çalışanların tatil yapmak zorunda kalması durumunda, bir çalışanın, çalışanın varlığına bağlı olarak hileli bir program oluşturma olasılığı daha düşük olacaktır (örneğin, dolandırıcılığın sürekliliğini veya gizliliğini korumak için). Çalışanın varlığı, şema için gerekli olmasa bile, gerekli tatiller, çalışanın bulunmaması durumunda keşfedilmekten korkabileceği için zimmete geçirmeyi caydırıcı olabilir.

**Arkaplan Araştırmalar:** Geçmiş araştırmalar, gelecekteki performansın potansiyel risklerini gösterebilecek geçmiş performansları ifşa edebilir. Terfi veya güven pozisyonuna geçme olarak değerlendirilen tüm çalışanların geçmiş araştırmaları yapılmalıdır; Bu tür soruşturmalar, çalışanın gerçekten hassas bir pozisyona yerleştirilmesinden önce yapılmalıdır. Hassas pozisyonlar için değerlendirilen iş başvurusunda bulunanlar ayrıca olası sorunlar için araştırılmalıdır. Devlet sınıfı projelere dahil olan şirketler, çalışanlar için gerekli güvenlik iznini elde ederken bu soruşturmaları yapmalıdır.

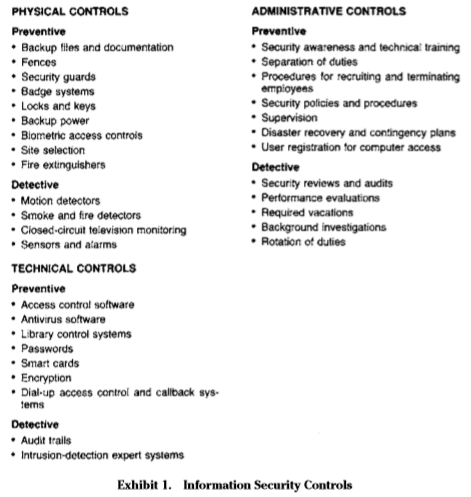
**Görevlerin Dönmesi:** Zorunlu tatiller gibi, görevlerin döndürülmesi (yani, çalışanları rastgele aralıklarla bir işten diğerine taşımak) dolandırıcılığın önlenmesine yardımcı olur. Ek bir yarar, dönen görevlerin bir sonucu olarak, çalışanların hastalık, tatil veya fesih durumunda birbirlerinin işlevlerini yerine getirmeleri için çapraz eğitimli olmalarıdır.

**ÖZET**

Bilgi güvenliği kontrolleri fiziksel, teknik veya idari olarak sınıflandırılabilir. Bunlar ayrıca önleyici ve dedektif kontrollere ayrılmıştır. Ek 1, bu bölümde tartışılan kontrolleri listeler.

Kuruluşun gizliliğini, bütünlüğünü ve kullanılabilirlik gereksinimlerini belirlemek için kuruluşun güvenlik politikası gözden geçirilmelidir. Güvenlik politikasında belirtildiği gibi gerekli bilgi korumayı sağlamak için uygun fiziksel, teknik ve idari kontroller seçilebilir.

Kullanıcıların güvenlik kontrollerini makul görmesini sağlamak ve kontrollerin verimliliği aşırı derecede engellememesini sağlamak için önleyici ve dedektif kontrol önlemleri arasında dikkatli bir denge kurulmalıdır. Belirli bir bilgi işlem ortamı için en uygun fiziksel, teknik ve idari kontrollerin kombinasyonu, nicel bir risk analizi yapılarak belirlenebilir. Bu genellikle pahalı, sıkıcı ve sübjektif bir süreç olduğu için, ancak gerekli bakım standardını karşılama olarak adlandırılan alternatif bir yaklaşım sıklıkla kullanılır. Uygun bakım standardını karşılayan kontroller, benzer koşullar veya ortamlarda çoğu kuruluş tarafından sağduyulu sayılacak olanlardır. Uygun bakım standardını karşılayan kontroller genellikle makul bir maliyet için hazırdır ve kuruluşun güvenlik politikasını destekler; en azından bireysel hesap verebilirlik, denetlenebilirlik ve görevlerin ayrılmasını sağlayan kontrolleri içerir.



**TEKNOLOJİ VE GİZLİLİK ÇATIŞTIĞINDA**

*Edward H. Freeman*

**Sonuç**

Sivil özgürlükçüler, bilgisayar ve iletişim teknolojisinin bireylerin kişisel gizliliği ve ifade özgürlüğü için ciddi bir tehdit oluşturduğunu düşünüyor. Bazıları, kişisel verilerin ele alınmasında hesap verebilirlik için etkili bir yasal zemin sağlamak ve bireyleri telafi etmek ve telafi etmek için prosedürler sağlamak üzere yasaları savunur. Bilgi otoyolunun geliştirilmesi kişisel mahremiyeti daha da tehlikeye atabilir.

**Ele Alınan Sorunlar**

Veri şifreleme, ek bilgi olmadan anlaşılamayan mesajları hazırlamak için kullanılan yöntemleri ifade eder. Devlet kurumları, özel şahıslar, sivil özgürlükler ve bilgisayar endüstrisi, bireysel ve toplumsal hakları güvence altına alacak veri şifreleme yöntemleri geliştirmek için çalıştılar.

Clinton yönetiminin şifreleme teknolojisi için yeni standartlar önerdiği - Clipper Chip - bireyin veri güvenliği konusundaki endişesine ve hükümetin kolluk kuvvetlerine olan ilgisinin cevabıydı. Yasalara uymayan vatandaşlar ihtiyaç duydukları şifrelemeye erişebilecek ve suç unsuru yasadışı faaliyetlerini gizlemek için şifreleme kullanamayacaktır.

**Şifreleme ve Gizli Mesajlar**

Şifreleme, güvenli ve gizli iletişim bilimidir. Bu güvenlik, gönderenin yalnızca gönderen ve yetkili alıcı tarafından bilinen bir bilgi parçası olan gizli bir anahtar kullanarak şifreli bir mesaja dönüştürmesini sağlar. Yetkili alıcı gizli bilgiyi kurtarmak için şifreyi çözebilir. Yetkisiz kişiler bir şekilde kodlanmış mesajı alırlarsa, anahtarın bilgisi olmadan kodunu çözemezler. Kriptografiyi yazışma için ilk kaydedilen kullanımı, 2500 yıl önce Spartalılar tarafından yaratılan Skytale oldu. Skytale, etrafına bir papirüs şeridinin sıkıca sarıldığı ahşap bir kadrodan oluşuyordu. Gizli mesaj parşömen üzerine personelin uzunluğu ile yazılmıştır. Parşömen daha sonra çözüldü ve yoluna gönderildi. Bağlantısız harfler, parşömen ilk çalışanlarla aynı büyüklükte bir ahşap elemanının etrafına sarılmadığı sürece hiçbir anlam ifade etmedi.

Mesajları kodlama ve kod çözme yöntemleri, savaş stratejilerinde her zaman bir faktör olmuştur. II. Dünya Savaşı sırasında Japon şifrelerini kıran Amerikan çabası, Müttefik stratejisinde önemli bir rol oynadı. Savaşın sonunda, kriptografi ve mahremiyet meseleleri, büyük ölçüde dış iletişimleri rutin olarak izleyen Ulusal Güvenlik Ajansı gibi kuruluşların izlediği hükümetin çıkarları meselesi olarak kaldı.

Günümüzde veri tabanları, her bireyin mali durumu, sağlık geçmişi ve satın alma alışkanlıkları hakkında kapsamlı bilgiler içermektedir. Bu veriler genellikle ucuz bir kişisel bilgisayar ve modem kullanarak telefon şebekeleri tarafından düzenli olarak aktarılır veya erişilebilir hale getirilir.

Hükümet ve özel kuruluşlar, kişisel mahremiyeti korumak için belirli standartların karşılanacağının farkına varır ve bireyler bekler. Örneğin:

* Saklanan veriler yalnızca bu bilgiyi bilmesi gereken kişi, kuruluş ve devlet kurumları için mevcut olmalıdır. Bu tür bilgiler, ilgilinin izni olmadan başkalarına (örneğin, müşterinin işverenine) sunulmamalıdır.
* Kuruluşlar bir veri tabanından alınan bilgilere dayanarak karar verdiğinde, bu kararlardan etkilenen bireyin veri tabanını inceleme ve yanlış ya da yanıltıcı olan herhangi bir bilgiyi düzeltme ya da düzeltme hakkına sahip olması gerekir. Bilginin yanlış kullanılması, bireyin istihdamı, sigortası ve kredisini tehdit edebilir. Önceki bir işlemin gerçekleri anlaşmazlık içeriyorsa, bireyler anlaşmazlığın kendi taraflarını açıklayabilmelidir.
* Sıkı anayasal ve adli kurallara ve kısıtlamalara göre, devlet kurumları ceza soruşturmaları kapsamında gizlice bilgi toplama hakkına sahip olmalıdır.

**Mevcut Mevzuat**

**1974 Gizlilik Yasası**

1974 Gizlilik Yasası, özellikle hükümet ve finansal faaliyetlerle ilgili olarak, bu sorunların bazılarına değindi. Kongre, bir bireye gizlilik istilasına karşı koruma sağlamak için Gizlilik Yasasını kabul etti. Gizlilik Yasası uyarınca, bireyler federal bir kurum veya büro tarafından tutulan hangi kayıtların onlar için önemli olduğuna karar verir. Bu verilerin yalnızca bilgilerin toplandığı amaçlar için kullanılması konusunda ısrar edebilirler. Bireyler bilgileri görme ve kopyalarını alma hakkına sahiptir. Gerektiğinde hataları düzeltebilir veya önemli ayrıntılar ekleyebilirler.

Federal kurumlar bilgiyi düzenli tutmalı ve böylece hazır bulundurulmalıdır. Sadece yasal amaçlar için kullanarak doğru ve güncel tutmaya çalışmalıdırlar. Bir kişinin Kanun uyarınca haklarının ihlal edilmesi durumunda, bu kişi federal bölge mahkemesinde tazminat davası açabilir ve kurumu hukuka uymaya yönlendiren bir mahkeme emri verebilir.

**1970'lerin Adil Kredi Raporlama Kanunu**

1970'lerin Adil Kredi Raporlama Yasası, tüketici raporlama ve kredi kuruluşlarının dosyalarındaki bilgileri etkilenen tüketicilere ifşa etmelerini gerektirir. Tüketiciler dosyalarında görünebilecek her türlü bilgiyi sorgulama hakkına sahiptir. Tüketiciden yazılı talep üzerine, ajans, o kişinin dosyalarında bulunan herhangi bir öğenin eksiksizliğini veya doğruluğunu araştırmalıdır. Ajans daha sonra bilgileri kaldırmalı veya tüketicinin anlaşmazlığın niteliğini belirten kısa bir açıklama yapmasına izin vermelidir.

Araştırmacılar, kişisel verileri ve iletişimleri yasa dışı müdahaleden korumak için karmaşık yöntemler geliştirmeye devam ediyor. Özellikle, milyarlarca doların elektronik olarak aktarıldığı Elektronik Fon Transfer sistemlerinin geliştirilmesi, bilgisayarlı iletişimin doğru ve gizli kalması gerektiğini vurguladı.

**Gizlilik Hakları**

Kısacası, bilgisayar ve iletişim teknolojisindeki hızlı gelişmeler, bireyin gizlilik hakkına yeni bir boyut getirmiştir. Günümüz bilgisayarlarının gücü, özellikle kayıt tutma ile ilgili olarak, kişisel gizlilik haklarını imha etme potansiyeline sahiptir.

Verilerin çoğu başlangıçta meşru ve uygun nedenlerden dolayı toplanırken, “bu büyük kişisel bilgi deposunun varlığı yanlış kullanım için gizli bir davet teşkil eder. “Sloan, I.J., ed., Teknolojik Bir Toplumda Gizlilik Hakları Kanunu (Dobbs Ferry, NY, Oceans Publications, 1986).”

Kişisel özgürlük, yalnızca fiziksel kısıtlama özgürlüğünü değil, aynı zamanda yalnız bırakılma ve başkalarının veya toplumun haklarına saygı duyulduğu sürece, o kişiye en uygun şekilde yönetme hakkını da içerir. Gizlilik kelimesi Anayasa'da bile görünmüyor. Kurucular, Haklar Taslağını hazırladıklarında, hiçbir belgenin Amerikan halkına verilen tüm hakları içeremeyeceğini fark ettiler.

İlk sekiz Değişiklikte belirli haklar listelendikten sonra, Kurucular, “Bu Anayasadaki belirli hakların sayımı, halkın elinde tuttuğu başkalarının reddetmesi veya hakaret etmemesi için yorumlanamaz” şeklinde ilan edilen Dokuzuncu Değişikliği hazırladılar. özellikle Anayasada tanımlanmadı. Mahkemeler, birçok hakın Anayasa'da özellikle belirtilmediğini, ancak belirli hükümlerden alındığını belirtti. Yargıtay, bazı değişikliklerin zaten gizlilik haklarını genişlettiğine karar vermiştir. Dokuzuncu Değişiklik daha sonra gizlilik hakkını kapsayacak şekilde yorumlanabilir.

**1934 Federal İletişim Kanunu**

Telefon ve telgrafları gizli dinleyicilerden koruyan federal yasalar, öncelikle 1934 tarihli Federal İletişim Yasası'ndan türetilmiştir. Kanun, bu tür iletişimleri göndermekle ilgilenen tarafların, içeriği ile ilgisi olan herhangi bir şeyi yayınlamasını veya yayınlamasını yasaklamaktadır. Bir istisna yapar ve mahkemenin meşru bir mahkeme celbi yayınlamış olup olmadığını açıklama izni verir. Yasa dışı bir telgrafla toplanan hiçbir materyal kabul edilemez ve federal mahkemelerde delil olarak sunulmayabilir.

**Veri Şifreleme Standardı**

Bilgisayar veri koruma şifreleme prosedürlerini belirten Ulusal Standartlar Bürosu Veri Şifreleme Standardı (DES), 1977'den beri federal bir standart olmuştur. DES algoritmasının kullanımı, Federal Rezerv Sisteminin üye bankaları tarafından yürütülenler de dahil olmak üzere, Elektronik Fon Transferini içeren ABD hükümetinin tüm finansal işlemleri için zorunlu hale getirildi.

DES, donanıma uygulandığında yüksek hızlarda çalışan, karmaşık, doğrusal olmayan bir şifreleme algoritmasıdır. DES algoritması, 56 bit anahtarlama parametresi eylemi altında 64 bit düz metin, 64 bit şifreleme metnine dönüştürür. Anahtar, algoritma tarafından doğrudan kullanılan 56 bitin her biri rastgele olacak şekilde üretilir. Şifreli veri yetkilendirilmiş bir kullanıcı grubunun her üyesi, onu kullanmak için verileri şifrelemek için kullanılan anahtara sahip olmalıdır. Bu teknik algoritmayı güçlendirir ve analize karşı dayanıklı kılar.

**Geleneksel Veri Şifreleme Yöntemlerindeki Loopholes**

DES, dönüşümü kontrol eden ve bilgileri şifrelenmiş koda dönüştüren 64 bit bir anahtar kullanır. Neredeyse sonsuz sayıda olası anahtar vardır, bu nedenle en hızlı bilgisayarların bile tüm olası anahtarları denemek için yüzyıllara ihtiyacı olacaktır.

Geleneksel şifreleme yöntemlerinde belirgin bir boşluk vardır: mesajları kodlamak ve kodlarını çözmek için tek bir anahtara bağımlı olmaları. Kodlanmış mesajların gizliliği her zaman dekoder anahtarının ne kadar dikkatli tutulduğunun bir fonksiyonudur. Ancak, insanlar mesaj alışverişinde bulunduğunda, anahtarı değiştirmenin bir yolunu bulmaları gerekir. Bu hemen anahtarı durdurma için savunmasız hale getirir. Şifreleme büyük ölçekte kullanıldığında sorun daha karmaşıktır.

**Diffle'nın Çözümü**

Bu sorun teorik olarak yaklaşık 20 yıl önce, Whitfield Diffle adlı bir MIT öğrencisi bu boşluğu tıkamak için yola çıktığında çözüldü. Diffle'ın çözümü her kullanıcıya iki ayrı anahtar, bir açık anahtar ve bir de özel anahtar vermekti. Açık anahtar yaygın olarak dağıtılabilir ve özel anahtar yalnızca kullanıcı tarafından biliniyordu. Her iki tuşla kodlanmış bir mesaj diğeriyle deşifre edilebilir. Bir kişi birisinin ortak anahtarıyla karıştırılmış bir mesaj gönderirse, yalnızca o kişinin özel anahtarıyla kodu çözülebilir.

**Clipper Tartışması**

1993 yılının Nisan ayında, Clinton yönetimi, Ulusal Güvenlik Ajansı ile geliştirilen şifreleme teknolojisi için yeni bir standart önerdi. Yeni standart Escrowed Encryption Standard adlı bir plandır. Standartlara göre, bilgisayar yongaları bilgileri şifrelemek için Skipjack adlı gizli bir algoritma kullanır. Clipper Chip, ses iletişimini şifrelemek için tüm telefonlara, bilgisayar modemlerine ve faks makinelerine kurulmak üzere tasarlanmış yarı iletken bir cihazdır.

**Clipper Chip**

Clipper Chip, 80-bit şifreleme şeması kullanan ve normal bir kullanım ömrü içinde günümüz bilgisayarlarıyla çatlamak imkansız olduğu düşünülen güçlü bir algoritmayı birleştiriyor. Çipte ayrıca yalnızca devlet kurumları için mevcut olacak gizli hükümet ana anahtarları da var. İletişimi engellemek için mahkeme emri şeklinde uygun yetkilendirme gerekli olacaktır.

Geleneksel veri şifreleme yongaları ve Clipper Chip arasındaki fark, Clipper'ın bir kanun uygulayıcı erişim alanı (LEAF) içermesidir. LEAF, kullanıcının verileriyle birlikte iletilir ve hükümetin ana anahtarı altında şifrelenmiş olan kullanıcının bireysel yongasının ve kullanıcının anahtarının kimliğini içerir. Bu, gizlice dinleyenlerin, kullanıcının anahtarını bularak kodu kırmasını engelleyebilir. Yetkili bir kurum bireysel çipin kimliğini bildiğinde, doğru ana anahtarı geri alabilir, kullanıcının anahtarının kodunu çözmek için kullanabilir ve böylece orijinal şifreli bilginin kodunu çözebilir.

**Uzun Anahtar**

Clipper, 1.024 değerde olabilecek uzun bir anahtar kullanır. Clipper'ın kodunu kırmanın tek yolu mümkün olan her anahtarı denemektir.

Tek bir süper bilgisayarın, Clipper'ın olası tüm anahtarlarını kullanması bir milyar yıl alacaktır. Clipper-Chip planının rakipleri birkaç defa uygulanmasını eleştirdi:

* Teröristler ve uyuşturucu satıcıları, Clipper Chip'e sahip olmaları durumunda telefonları rahatsız ederdi. Ayrıca, kendi çiplerini kullanabilirler.
* Yabancı müşteriler, iletişiminin ABD devlet kurumları tarafından ele geçirilebileceğini bilselerdi, Amerikan üreticilerinden ekipman satın almazlardı.
* “Arka kapı” sisteminin bütünlüğü, acımasız federal çalışanlar tarafından tehlikeye sokulabilir.
* Uzak ihtimal, uzman bir kriptologun bir şekilde kodu kırabilmesidir.

**Tavsiye Edilen Eylem**

Bilgisayar endüstrisi ve sivil liberterlerin muhalefetine rağmen, devlet kurumları, sınıflandırılmamış iletişim için Clipper teknolojisinde aşama yapıyor. Clipper'ın ticari kullanımı hala tamamen isteğe bağlıdır ve devlet dışındaki herhangi bir kuruluş tarafından benimseneceğine dair hiçbir garanti yoktur. Yine de, binlerce Clipper donanımlı telefon, devlet kullanımına açık durumda. Adalet Bakanlığı, polis ve FBI’nın emri olmadan konuşmaları dinlemesini önleyecek önerileri değerlendiriyor.

Gizlilikle ilgili bu endişelere yönelik olası bir çözüm, şifre çözme anahtarını iki veya daha fazla bölüme ayırmak ve ayrı devlet kurumları için mütevelli heyeti vermek.

Teoride bu, bir mesajın ele geçirilmesinden önce birkaç kişi ve kurumun işbirliğini gerektirecektir. Bu çözüm gizli bir ceza soruşturması yapmak için gereken gizliliği tehlikeye atabilir, ancak Adalet Bakanlığı bunun uygulanabilirliğini araştırıyor.

Hiçbir veri şifreleme yöntemi, bireysel mahremiyeti ve toplumun suç faaliyetlerini durdurma arzusunu her zaman koruyamaz. Elektronik Fon Transfer sistemleri ve bilgi otoyolu, özel haberleşmeye olan ihtiyacı her zamankinden daha önemli hale getirdi. Toplumun uyuşturucu ve terörle ilgili sorunları, bireyin mahremiyet hakkı, toplumun kendisini koruma ihtiyacı ve herkesin Büyük Kardeş hükümet araçları korkusuyla ilgili hassas dengeyi vurgulayarak sorunları karmaşıklaştırmaktadır.

**Yazar Biyografileri**

**Edward H. Freeman:** Edward H. Freeman, West Hartford CT'de avukat, öğretmen ve öğretim görevlisidir ve en son büyük bir sigorta şirketi olan veri işleme alanında 15 yıllık bir deneyime sahiptir. Central Connecticut State University'de yarı zamanlı bir öğretim üyesidir.

**EK KONU**

**EAVESDROPPİNG NEDİR?**

Eavesdropping, Türkçeye ‘Telekulak’ olarak çevrilmektedir. İlk olarak İngiltere’de 1769 yılında çıkan kanun ile birlikte asıl manası olan ‘Saçaklı Saldırı’ olarak kayıtlara geçmiştir. Böyle anılmasının sebebi, eskiden insanlar birbirlerini dinlemek için evlerinin saçaklarına gizlenir ve oradan içeride olup biteni dinlemeye çalışırlarmış. Günümüzde ise eavesdropping; akıllı telefonlar, bilgisayarlar, güvensiz ağ bağlantıları, SSL sertifikası veyahut SSH(güvenli kabuk)’ ı bulunmayan siteler aracılığıyla kötü niyetli kişi veya kişiler tarafından dinlenilmesidir. Özet olarak söyleyecek olursak, insanın özeli kabul edilen cihazlara, yazılım veya program yüklenerek, uzaktan erişim sağlayıp istem dışı olarak dinleme yapılmasıdır.

Bir ağ veya kanal üzerinden iletilen verinin, kötü niyetli üçüncü kişiler tarafından araya girilerek alınmasıdır. Bu saldırı tipinde, hatta kaynaktan hedefe giden verinin arada elde edilip, değiştirilerek hedefe gönderilmesi bile mümkündür. Saldırının sanıldığının aksine çok farklı uygulama alanı bulunmaktadır. Hiç bir bilgisayarla etkileşimi olmayan tek başına çalışan bir bilgisayar bile, mikroçip, ekran veya yazıcı gibi elektronik parçalarından yayılan elektrik veya elektromanyetik yayılım takip edilerek gizlice dinlenebilir. Bu cihazların bu tür dinlemelere olanak vermemesi için, Amerikan hükümeti 1950’li yılların ortasından başlayarak TEMPEST adında bir standart geliştirmiştir.

**Aktif Eavesdropping Saldırısı**

Aktif Eavesdropping ataklarında, kötü niyetli kişi, istemci ile sunucu arasında değişiklik gösterilerek ilgili yazılım veya program aracılığı ile sunucuyu veyahut istemciyi kendi istediği bir konuma yönlendirebilmektedir. Bunu yapmanın en bilindik yöntemi ise spoofing ile aldatma saldırısı düzenlemektir.

**Pasif Eavesdropping Saldırısı**

Pasif Eavesdropping ataklarında dinlenildiğinizi, izlenildiğinizi çoğu zaman fark edemeyebilirsiniz. Bunun için özel programların olmasının yanı sıra kötü niyetli bir kişi size sosyal medya üzerinden göndereceği bir link veyahut cihazınıza yükleyebileceği virüs ile sizlerin cihazınız üzerinde yaptığı her hareketi gözaltına alabilir.

**Wireshark ile Pasif Eavesdropping**

Pasif dinleme ve izlemeyi gerçekleştirmek için herkesin erişebileceği, Windows ve Linux için uyumlu bir program olan Wireshark idealdir. Bu program aracılığı ile IP adresini belirlediğiniz bir kurbanın network trafiğinden, SSL sertifikasına hatta portlarına kadar takip edebilirsiniz. Wireshark programının birçok özelliğinin bulunmasının yanı sıra grafik arayüzü ile de temel düzeyde bilgisi olan kullanıcıların çok kolay kullanabileceği bir ağ analizi aracıdır. Bu özelliklerinden bazılarını sıralayacak olursak;

* Belirlediğiniz hedefteki paketleri tutarak sizlere sunabilir.
* İstatistiksel özellikleri ile kendinize özel belirlediğiniz grafikleri size sunar.
* Filtreleme özelliği ve belirlediğiniz metriklerin renkler ile ayrılmasını sağlayarak sizleri meşakkatten kurtarır.
* Ağda olan biten her şeyi bize gösterir.
* Ücretsiz olması ve buna rağmen sunduğu özellikler ile gerçekten sağlam ve kesinlikle güvenilirdir.

Wireshark ile kendi ağ trafiğinizi de izleyip analizler gerçekleştirebilirsiniz. Bilgisayarla ve internetle ilgisi olan herkesin bu ağ analiz aracını kullanması kendisi için gereklidir. Ağ trafiğinizde ne olup ne bittiğini, anormal bir durumun olup olmadığını bu sayede görebilir ve çözebilirsiniz.

**Eavesdropping Saldırılarından Nasıl Korunulmalıdır?**

Fiziksel Dünyada her yaptığınız ve her söylediğinizin başkaları tarafından dinlenilmesinin, izlenilmesinin ne kadar sinir bozucu olduğunu tahmin edebiliyorsunuzdur. Bir de bunun dijital dünyada başınıza geldiğini veya gelebileceğini düşünün. Durum yine aynı şekilde can sıkıcıdır. Peki, bunu engellemek imkânsız mı? Elbette ki hayır, değil. Eavesdropping saldırılarından korunmanın yolları basittir.

* Genel olarak kullandığınız veya E-Ticaret siteleri üzerinde mutlaka SSL sertifikası(https://) veya SSH ı bulunmasına özen gösterin. SSL sertifikası, istemci ile sunucu arasındaki verinin 128 ile 256 bit arasında şifreleme yapmasını sağlar ve girdiğiniz bilgilerin 3. kişiler tarafından izlenilmesini engeller.
* Genel Wi-Fi ağlarından uzak durun. Bu ağlar, düpedüz tuzaktır. Herkesin bağlanabildiği ağlarda kolayca veri izlemesi yapılmasının yanı sıra, etkileşim kurduğunuz cihaz üzerinden işlemler gerçekleştirilebilir.
* Bilmediğiniz keza güvenmediğiniz hiçbir linke tıklamayın veya girmeyin.
* Kullandığınız cihazların güncellemelerini kontrol edin ve her zaman güncel olmasına özen gösterin. Çünkü yeni getirilen güncellemeler ile eski sürümün açıkları paylaşılmaktadır ve nelerin düzeltildiği ilan edilmektedir.
* Sitenizin güvenliğini ve güncelliğini tam olarak sağlayın.
* XSS açıklarına dikkat etmelisiniz.

Spoofing ile cihazınıza veya kullandığınız bir siteye kök işlem saldırısı yapabilirler ve bu işlem çalışma performansını vs hiçbir şekilde etkilemediği için siz bunun farkına dahi varamayabilirsiniz. Bundan dolayı yukarıdaki maddelere özen göstererek eavesdropping saldırı türlerinden uzak kalabilirsiniz.

**KAYNAKLAR**

[1] <https://www.cozumpark.com/bilgi-g-venli-i-ve-genel-g-venlik-kavramlar-b-l-m-2/>

[2] <https://www.techopedia.com/definition/13612/eavesdropping>

[3] <https://www.dogukankaradag.com/eavesdropping-attack-ile-desifre-olmak/>

[4] Gürol CANBEK, Şeref SAĞIROĞLU (2007). *BİLGİSAYAR SİSTEMLERİNE YAPILAN SALDIRILAR VE TÜRLERİ: BİR İNCELEME*

[5] Merve YÜKSEL, Nihat ÖZTÜRK (2017). *SIP Saldırıları ve Güvenlik Yöntemleri*

# [6] Z Zhang, Z Man, Y Li (2004). *Improving Wójcik's eavesdropping attack on the ping–pong protocol*

# [7] Henning Weier, Harald Krauss, Markus Rau, Martin Fürst, Sebastian Nauerthand Harald Weinfurter (2011). *Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors*

# [8] F. Maggi, Alberto Volpatto, Simone Gasparini, Giacomo Boracchi, Stefano Zanero (2011). *A fast eavesdropping attack against touchscreens*

[9] İzzet Gökhan ÖZBİLGİN (2003). *BİLGİ TEKNOLOJİLERİ DENETİMİ VE ULUSLARARASI STANDARTLAR*

[10] Mustafa GÜLMÜŞ (2011). *Kurumsal bilgi güvenliği yönetim sistemleri ve güvenliği*

[11] Emine TUĞ İLÇİN, Ş. Feyza ADAK, Hüseyin ÇAKIR (2012). *Bilişim Güvenliği Tedbirleri ve TKDK Kurumunda Uygulama Örneği*