T.C. ATATÜRK ÜNİVERSİTESİ

MÜHENDİSLİK FAKÜLTESİ

PHYSİCAL SECURİTY: CONTROLLED ACCESS AND LAYEREDDEFENSE

COMPUTİNG FACİLİTY PHYSİCAL SECURİTY

HABİBE AKSAKAL 150707025

LİSANS BİLGİSAYAR MÜHENDİSLİĞİ

2019

T.C. ATATÜRK ÜNİVERSİTESİ

MÜHENDİSLİK FAKÜLTESİ

FİZİKSEL GÜVENLİK: KONTUROLLÜ ERİŞİM VEKATMANLI SAVUNMA

BİLGİ İŞLEM TESİSİ FİZİKSEL GÜVENLİK

HABİBE AKSAKAL 150707025

LİSANS BİLGİSAYAR MÜHENDİSLİĞİ

2019

**ÖZET**

**FİZİKSEL GÜVENLİK: KONTUROLLÜ ERİŞİM VEKATMANLI SAVUNMA**

**BİLGİ İŞLEM TESİSİ FİZİKSEL GÜVENLİK**

**Habibe AKSAKAL**

**Lisans Tezi, Bilgisayar Mühendisliği Danışman: Prof. Dr. Abdulsamet HAŞILOĞLU Mayıs 2019, 15 Sayfa**

Bilgisayar Mühendisliği alanındaki teknolojik gelişmeler bilgi sistemleri üzerinde işlenen ve paylaşılan bilginin boyutunu hızla artırmaktadır. Kamu kurum ve kuruluşları bu gelişmeleri takip ederek bilgi sistemleri sayılarını arttırmakta, temel görevlerini diğer kamu kurum ve kuruluşları ile bilgi paylaşım esasına göre bu sistemlerin üzerinde sürdürmekte ve vatandaşlara sunmaktadır. Özel sektörde de durum pek farklı değildir. Internet bankacılığı ile başlayan hizmetler bankacılık dışında hizmet veren firmaların artması ve güçlenmesi ile internet üzerinden her gün daha fazla kişi tarafından kullanılmaktadır. Bu nedenle bilgi sistemleri üzerindeki bilginin güvenliği ve hizmetlere erişilebilirlik bu hizmetleri veren kamu ve özel kurum ve kuruluşları için önem verilmesi gereken bir konu olmaktadır. Bu çalışmanın amacı bilgi sistemleri güvenliği kavramının araştırılarak sınırlarının tanımlanması ve mantıksal güvenlik alanında yararlı olabilecek güvenlik yazılımlarının kurum ve kuruluşlar tarafından nasıl kullanılabileceğinin özetlenmesidir.

**İÇİNDEKİNLER**

[1. GİRİŞ 6](#_Toc9949859)

[2.FİZİKSEL GÜVENLİK (Physical Security) 6](#_Toc9949860)

[3.GÜVENLİK: KONTROLLÜ ERİŞİM 7](#_Toc9949861)

[4.KATMANLI SAVUNMA 7](#_Toc9949862)

[5.FİZİKSEL GÜVENLİK TEKNOLOJİSİ 8](#_Toc9949863)

[5.1.Güvenlik bileşenleri 8](#_Toc9949864)

[5.1.1.Kilitler 8](#_Toc9949865)

[5.1.2.Bariyerler 9](#_Toc9949866)

[5.1.3.Alarm 9](#_Toc9949867)

[5.1.4.Kapılar 9](#_Toc9949868)

[6.FİZİKSEL GÜVENLİĞİ BT GÜVENLİK POLİTİKASI İLE BÜTÜNLEŞTİRME 10](#_Toc9949869)

[7.BİLGİ İŞLEM MERKEZLERİ 10](#_Toc9949870)

[8.BİLGİ İŞLEM MERKEZİ EVRİMİ 11](#_Toc9949871)

[9.KORUYUCU ÖNLEMLER 12](#_Toc9949872)

[10.ÇEVRESEL ENDİŞELER 12](#_Toc9949873)

[10.1.Topluluk 12](#_Toc9949874)

[10.2.Doğanın Davranışları 13](#_Toc9949875)

[10.3.Diğer Dış Riskler 13](#_Toc9949876)

[10.4.Tesis 14](#_Toc9949877)

[10.5.Koruma Katmanları 14](#_Toc9949878)

[11. KAYNAKLAR 14](#_Toc9949879)

**SİMGELER VE KISALTMALAR DİZİNİ**

**Simgeler**

**Kısaltmalar**

BT Bilgisayar Teknikeri

ISO Uluslararası Standartlar Teşkilâtı

COBIT Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri

PCI DSS Payment Card Industry Data Security Standardı

BDDK Bankacılık Düzenleme ve Denetleme Kurumu

# 1. GİRİŞ

BT güvenlik uygulayıcısının işinin her yönü, tanımlama, uygulama vebilgiye erişimin izlenmesidir. Burada fiziksel erişim de bulunur. Ne zaman, ne kadar gibi kavramlar. BT güvenlik uzmanının olması gereken kavramlardır.BT güvenlik uzmanının uzman olması gerekmez, başka biri bu rolü yerine getirir ancak etki, politika, stratejiler kavramlarını ve fiziksel korumanın sınırlarını ve faydalarını da dikkate almalıdır.Temelde, katmanlı, çok disiplinli bir yaklaşım sağlayabilir. Kontrollü erişim güvenliktir.Çoğu bilgi güvenliği uygulayıcısı, bilgisayarın ve

telekomünikasyon güvenliği, fiziksel güvenliği başka bir departmana bırakır.

Fiziksel erişim kontrolleri ve bilgi işlem kaynaklarının korunma önlemleri, çevrelenmiş bir güvenlik programının temel bileşenleridir. Ancak, tüm tesisin korunması refah için daha da önemlidir. Örneğin; İşyerinde çalışanların ve ziyaretçilerin. Ayrıca, çalışma saatleri sırasında veya sonrasında tesisdeğerli veriler genellikle katılımsız bırakılan makineleri kullanarakmasaüstü uygulamalara erişim sağlanabilir. Tümüne ücretsiz erişimrakipler veya sanayi yapan insanlar için muazzam bir varlık olacaktır. Ayrıca şirkete zarar vermek isteyen hoşnutsuz çalışanların veya ortakların da büyük bir riski vardır.

11 Eylül 2001’de Dünya Ticaret Merkezi’ne yapılan saldırıda da gösterildiği gibifark ettiğimizden daha büyük tehlikeler var. Dış tehlikeler, önceden düşünülenden daha muhtemel görünüyor.

Tesislere fiziksel erişim, ziyaretçiler üzerinde kontrol eksikliği ve tespit önlemlerinin eksikliği gibi eksikliklerden kaynaklanır. Böylece işyerleri ve çalışanlarımız tehlikededir. Ek olarak, şirketlerin küçülmesine neden olan ekonomik yavaşlamalar

Yerinden edilmiş çalışanlardan istihdam kaybına üzülebilecek riskler yaratabilir.

Fiziksel güvenlik, değerli bilgileri korumak için her zamankinden daha önemli ve daha değerlidir.

Akılcı maliyete karşı varlıkların değeri, çevrede algılanan tehditler gibi çeşitli faktörler ve daha önce uygulanmış olan koruyucu önlemler uygulanmalı ve fiziksel güvenlik planı geliştirilmelidir. Başarılı olmak için yönetimin yanı sıra çalışanlara da dikkat edilmeli onlar tarafından da güvenlik geliştirilmelidir. Ayrıca yapılan güvenlik uygulamaları ve çalışmalarıkuruluşun işini desteklemek içinperiyodik olarak gözden geçirilmeli ve denetlenmelidir. Eksikler varsa giderilmeli geliştirilmeli ve güncellenmelidir.

# 2.FİZİKSEL GÜVENLİK (Physical Security)

İşyerine yetkisiz erişimlerin engellenmesi ve bilgi varlıklarının hırsızlığa veya tehlikeye karşı korunmasıdır.

Örneğin, bina etrafına yüksek duvarlar ya da demirler yapılması, bina girişinde özel güvenlik ekiplerinin bulundurulması, önemli verilerin tutulduğu odaların kilitlenmesiya da bu odalara şifreli güvenlik sistemleri ile girilmesi gibi önlemler kullanılmaktadır.

# 3.GÜVENLİK: KONTROLLÜ ERİŞİM

Erişim kontrolü, bir kaynağa erişimin ve o kaynağın kullanımının kişilere yetkiler vererek ve kısıtlamalar getirerek sınırlanmasıdır. Örnek olarak, hassas bilgiler içeren kurumsal programlara erişimlerin uygun şekilde düzenlenmesi ve kullanıcıların uymaya zorlanması, veri tabanı ve sistem yönetim araçlarına ilgili BS personeli dışında erişimin engellenmesi ve sistem odasına sadece yetkili personelin girebilmesi verilebilir.Bilgi güvenliğinin sağlanmasında yüksek derecede önem taşıyan erişim kontrolleri, uluslararası standartlar ve yerel düzenlemelerde yoğun şekilde referanslanmaktadır. Erişim kontrollerine ilişkin maddeler içeren dokümanlardan bazıları aşağıda listelenmiştir.

− ISO 27002 Bilgi Güvenliği Yönetimi için Uygulama Prensipleri Standardı dokümanında 7 başlık altında 25 kontrol hedefi, − COBIT 4.1 dokümanında 3 ana başlık altında 7 kontrol hedefi, − PCI DSS dokümanının 12 gerekliliğinden 3 tanesi, − BDDK Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ’de 3 madde, − Ülkemizde pek çok kurumun uyum gerekliliği olan Sarbanes-Oxley yasasının 404. bölümü.

# 4.KATMANLI SAVUNMA

Katmanlı bir savunma, bir miktar fazlalık sağlayarak ve genişleterek erişim kontrollerine duyulan güveni arttırır. Fiziksel güvenlik için katmanlı bir savunma planlamanın detayları bu bölümün kapsamı dışındadır ve deneyimli bir fiziksel güvenlik uygulayıcısı tarafından ele alınmalıdır. Ancak, BT güvenlik uzmanı katmanlı bir savunmanın faydalarını, sağlayacağı ve sağlamayacağı güvenliği değerlendirebilmelidir. Katmanlı bir savunmayı planlayan kişi, üç temel ilkeye ayırır: genişlik, derinlik ve caydırıcılık.

Genişlik kullanılır, çünkü tek bir kontrol türü nadirenaçıkların hepsini ortadan kaldırır. Bunu ilk olarak tanıdık BT dünyasında ilişkilendirip, birinin verilere okuma erişimini kontrol etmeye karar verdiğini varsayalım. (Oturum açma şifresi kullanarak). Oturum açma şifresi, verileri veri yoluna gönderirse koruma sağlamaz. Bu nedenle farklı bir kontrol türü (yani şifreleme) ihtiyaç duyulan ek kapsamı sağlayacaktır. Fiziksel güvenlik aynı şekilde çalışır. Örneğin, bir kişinin bekleme modunda iken erişimini kontrol etmesi gerektiğini varsayalım. Tesis, bir ön kapıya, arka kapıya, büyük bir garaj kapısına ve açılmayan sabit pencerelere sahiptir. Kapılardaki kilitler içeriye doğru bir yol tipini kontrol eder ancak kırılabilir camlar için koruma yok.

İkinci ilke, derinlik, genellikle göz ardı edilir, ancak çoğu zaman bir katman için en önemli özelliktir. Güvenlik konusunda gerçekçi olmak için, birinin başarısızlığa inanması gerekir. Herhangi bir kontrol mükemmel değildir veer ya da geç başarısız olur. Böylece, derinlik için, bir geri döndürücü ölçü olarak ek erişim kontrollerinin katmanları eklenir.Temelde, tek duvar, arka arkaya birkaç duvar haline gelir. Tanıdık bir zeminde göstermek için, kullanıcı şifresine bir göz atılır. Parola sonsuza dek gizli kalmaz, genellikle tek bir gün için olmaz, çünkükullanıcıların bunları yazma veya paylaşma alışkanlığı vardır.

Fiziksel güvenlik için derinlik genellikle dış çevreden, nesnelerden uzakta olan alanlardan çalışır.

Korunacak nesnenin yakınındaki orta alana Teoride, her erişim kontrolü katmanı bir

merkeze doğru eş merkezli halka (çok az sayıda tesis tamamen yuvarlak olmasına rağmen). Katmanlar genellikle tanımlanırgerekçesiyle, binanın giriş ve dış cephelerinde, binanın katlarında, ofis odalarının,bireysel ofis ve dosya dolapları veya kasalar.

Caydırıcılık, üçüncü ilke, maliyet veya fizibilitesinin yeterli olduğu kontrolleri koymaktır. Yakalanmadan onları yenmektir.

# 5.FİZİKSEL GÜVENLİK TEKNOLOJİSİ

## 5.1.Güvenlik bileşenleri

### 5.1.1.Kilitler

Fiziksel güvenlik kontrolleri büyük ölçüde kilitlerden oluşur (profesyoneller tarafından kilitleme aygıtı olarak adlandırılır).İşlev açısından, günlük erişim kilitleri, mesai sonrası kilitler ve acil çıkış kilitleri vardır. Yetkili kişiler için gün kilitleri izin verir; kolay erişim - tuş takımı veya kart kaydırma gibi. Mesai sonrası kilitlerin kullanım amacı yoktursık sık açılıp kapanabilir ve çoğu zaman daha önemlidir. Örneğin; anahtar kilitleri, kilitli sürgü kilitleri,asma kilitler, kombinasyon asma kilitler veya yüksek güvenlikli şifreli kilitlerin kasalarda veya kasa kapılarında görüldüğü gibi.

Acil durum çıkış kilitleri bir yöne (yani, ateşten uzak) kolay erişime izin verir.

Ortak bir örnek, kamu tesislerinde acil durum çıkışlarında görülen “itme” veya "çarpma" çubuk tarzıdır.Sadece dışarı çıkmak için çubuğu itin, ancak bir geri almak için bir anahtar gerekiyor.Çeşitlere göre, kilitler mekanik veya elektrik olabilir. Mekanik bir kilit, elektrik gücü gerektirmez. Bir elektrikli kilit taşımak için elektrik gerektirir. Kilitleme mekanizması, genellikle solenoid denilen bir bileşen ilebir şaftın etrafındaki bir tel bobinden oluşur.Şaft, elektrik akımı bobinden akarken içeri veya dışarı hareket eder. Başka bir elektrikli kilit türü isebir kapıyı kapalı tutmak için büyük elektromıknatıs. Avantaj, kayda değer tutuş gücüne sahip az sayıda hareketli parçadır. Her gün insanların kendilerini kilitleme kimliklerini doğrulama (bir BT terimi kullanmak için) daha karmaşık hale geliyor. Geleneksel olarak, insanlar anahtar veya mekanik bir kombinasyon kullandılar. Şimdi şifreli kilitler var

Dahili mikroişlemcileri ve devreleri çalıştırmak için kadranı döndürdüğü zaman elektrik üreten. Ayrıca insanları tanımlamak için elektronik tuş takımları, bilgisayarlar, biyometri ve kart tuşları... Bu daha fazla olmasına rağmen

BT güvenlik uzmanına tanıdık bölge, hepsi bir kilitleme cihazını aktive etmekle kaynaşıyor. Toplu olarak, kapı kilitleme cihazlarıyla birleştirilmiş kimlik doğrulama, “kapı kontrol sistemi” olarak adlandırılır.

### 5.1.2.Bariyerler

Bariyerler; duvarları, çitleri, kapıları, direkleri ve kapıları içerir. Engellerin tasarımına şaşırtıcı miktarda teknoloji ve düşünce var. Engellerin arkasındaki fizik, bomba patlamaları, yangına dayanıklılık hesaplamaları içerebilir.

### 5.1.3.Alarm

Bariyerler ve onları doğrudan sabitleyen kilitler erişimi doğrudan kontrol eder. Alarmlar öncelikle bize bunu bildirmek için konumlandırılır. Alarmlar bize ne zaman bir eylem yapılması gerektiğini söyler.

Alarm zili polis departmanını arama gibi bir şeydir. Birkaç kontrolü izleyen bir tesis

birimlere “merkezi izleme” tesisi denir.Sensörler genellikle çevresel koşulları veya izinsiz girişleri algılar. Çevre koşullarısıcaklık, nem ve titreşimi içerir. Sıcaklık yalnızca yangına karşı koruma sağlamakla kalmaz, aynı zamanda bizi de uyarabilir.

Klima bir sunucu odasında başarısız oluyor. Nem, yağmurlar veya kırık su tesisatı nedeniyle su baskınlarını gösterebilir.Titreşimsensörleri hem çevresel sensörlerde, hem de hassas donanımı korumak için ve izinsiz girişlerde kullanılır

cam kırılma algılayıcıları veya tırmanmayı tespit etmek için çitler üzerinde bulunan dedektörler. Diğer izinsiz giriş sensörleri bir odadaki ısı veya ultrasonik ses değişikliklerini ölçerek hareketi ve insanı algılar. Aslında, birçok saldırı sensörü

gerçekten sadece insan etkinliği için yapılandırılmış çevresel sensörler.

### 5.1.4.Kapılar

Genellikle manyetik anahtarlarla izlenir. Kapıya bir mıknatıs monte edilmiştir ve bir anahtar yapılmıştır. İnce metal şeritlerin kapı çerçevesine monte edilir. Kapı kapandığında, mıknatıs metal şeritleri çeker kapalı, bir devrenin tamamlanmasıdır. (veya bir devreyi kırmak için onları açık iter). Bir alanın çevresi, bir kişi onlardan geçer. Üstünden geçen insanları tespit eden toprağa kablolar gömülebilir. Hayvanlar bu çevre sensörleri için yanlış tespit kaynağıdır. Birçok alarm sisteminin önemli bir özelliği, sensörlerin kontrol cihazıyla nasıl iletişim kurduğudur - kablosuz veya kablolu-. Kablosuz sistemler genellikle kurulumu daha ucuzdur, ancak radyo frekansı girişimine maruz kalabilir veya kasıtlı sıkışma. Kablolu sistemlerin kurulması pahalı veya pratik olabilir ancak oldukça güvenli bir şekilde yapılabilir, özellikle teller boru içindeyse. Kablolu veya kablosuz olsun, daha iyi sistemler bazı denetleyicinin sistemin bütünlüğünü izleme yöntemi. Sensörlerdeki bilgileri dikkate almayın. Böyle hayati bir işlev ile, bir kişinin kimlik doğrulamasının bazı yolları olmalı Kişinin alarm sistemini kapatma yetkisi. Önceki bölümdeki kilitler gibi, yöntemler Bunu yapmak temelde şifrelerden, herhangi bir bilgi sistemine kimlik doğrulaması yapmakla aynıdır. Akıllı kartlara biyometriye, aynı artı ve eksilere sahip.

# 6.FİZİKSEL GÜVENLİĞİ BT GÜVENLİK POLİTİKASI İLE BÜTÜNLEŞTİRMEK

Bilgiyi koruma politikaları hem fiziksel hem de BT güvenlik gereksinimlerini karşılamalıdır. Politika her ikisini de kapsamalıdır. Yaklaşımda tutarlı olmalı, ancak uygulamada her zaman aynı olmamalıdır. Örneğin, gizli proje bilgilerinin proje ortaklarına güvenli bir şekilde iletilmesini sağlamak için bir politika olduğunu varsayalım. Kağıt dünyası için mühürlü bir zarf yeterli olabilir; ancak dijital dünya için sağlam şifreleme gereklidir. Şüphesiz, dağıtım bisikletçisi bir zarfı açabilir ve içeriği görebilir.

Bununla birlikte, İnternet üzerinden veri gönderilirken, kişi onunla temasa geçebilir ve etik dışı bir insana neredeyse hiç bedel ödemeden inanılmaz hızlarda muazzam miktarlarda çoğaltılabilir hatta yeniden dağıtılabilir.

“Örneğin, yüksek seviyeli bir politika şöyledir: “Kullanıcılar ağ erişimi için benzersiz bir şekilde tanımlanmalıdır.” Bu, şifreler, parola makbuzları ve parola depolaması standartlarını ortaya koymaktadır.

# 7.BİLGİ İŞLEM MERKEZLERİ

Bilgisayar donanım ve yazılım olanakları ve başta veri hazırlama donanımı olmak üzere öngörülen bilgi işlem hizmetleri için gerekli tüm öteki yardımcı makinelerle donatılmış, yönetici insangücünün yanı sıra dizge çözümleyiciler, izlenceleyiciler, işletmenler vb. gibi bilişim insangücünden oluşan ve içinde bulunduğu örgüte ya da dışarıya bilgi işlem hizmeti sunmayı amaçlayan örgüt.

Bilgi işlem merkezleri yıllar içinde gelişti, ancak yine de önemli bilgi işlem varlıklarının bulunduğu alan olarak kaldılar.Farklı koruma derecelerine sahiptirler ve

yönetim algılarına ve içerdikleri varlıklara bağlı olarak koruyucu önlemler.

Teknik ekibin üyeleri genellikle mesai saatleri dışında bilgi işlem merkezi erişimi talep ediyorlar. Sistemleri yeniden başlatmanız gerekebilir. Yönetim üyeleri aynı zamanda erişim talep edebilirler çünkü şirket, şirket varlıkları üzerinde denetim kontrolü olmasını gerektirir. Ek olarak, bilgisayar odasına erişim

sistemlere hizmet veren satıcı ve müşteri mühendisleri gibi çalışanlara verilmemektedir. Takip etmek yetkili erişim ve minimumda tutulmasını sağlamak bilgi güvenliği için büyük bir görevdir.

# 8.BİLGİ İŞLEM MERKEZİ EVRİMİ

Büyük ana bilgisayarların olduğu günlerde, bilgi işlem merkezleri genellikle tüm binaları işgal etti; ilgili personel için. Bunlar, birçok kişinin ihtiyaç duyduğu merkezi bilgi işlem merkezlerinin günleriydi. bir dizi gerekli görevi yerine getirmek. Operatörlerin yazdırma işlemlerini yürütmesi, takması ve çıkarması gerekiyordu bantlar ve ana konsolu yönetin. İşlerin kurulması ve programlanması için üretim kontrol kadroları gerekiyordu. İçinde ek olarak, sistem programcıları ve bazı durumlarda sistem geliştiricileri için kadro istediler. Bilgisayar Güvenliği yönetimi zordu, ancak bazı kontroller işlevleri sürdürmek için fiziksel duvarlar yerleştirildi. ayrı. Bu büyük sistemlerden bazıları hala kalıyor; ancak, fiziksel bilgisayar odası görevleri azaltıldı otomasyon ve departman baskısı yoluyla. Dağıtılmış sistemler geliştikçe, sunucular sık ​​sık sistem yöneticileri tarafından yüklendi ve yönetildi. tüm sistem görevlerini yerine getirdi. Bu sistemlerin birçoğu, ofis ortamlarında çalışmak için oluşturulmuştur. ısı ve nem üzerinde sıkı çevresel kontroller için ihtiyaç. Sonuç olarak, sunucular ofislerde bulundu kilitli bir kapının arkasına yerleştirilmeyebilecekleri yer. Bu güvenlik gelişi ile daha da aşınmış Masaüstü bilgisayar, veriler ofis genelinde mevcut olduğunda. Birçok durumda, sunucular kendi ekipmanlarını kontrol etmek isteyen ve yapmayan çeşitli bölümlerde uygulanmış ve kurulmuş Bürokratik değişim kontrolleri, ters ibrazlar ve kontrol işlemleriyle bilgi işlem personeline geri dönmek istiyorlar. Son kullanıcı ihtiyaçlarına yavaş algılanan yanıt.Yerel ağlar ve dağıtılmış sistemler stratejik önem kazandıkça, daha büyük kullanıcı tabanları elde edildi, ihtiyaç duyuldu yazılım yükseltmeleri ve ara bağlantı, son kullanıcı departmanlarının yönetmesi ve kontrol etmesi zorlaştı sistemler Ayrıca, denetim departmanı olmayan güvenlik gereksinimleri olduğunu fark etti. Bu kritik sistemleri desteklemek için yerine getirildi. Bu, sistemlerin yeniden merkezileşmeye göç etmesine neden oldu kontrol ve merkezi bilgisayar odaları. Bu sistemler çevresel dalgalanmalara dayanabilse de, gereken sayıda sunucu gerekli ısıyı düşük tutmak ve kesintisiz güç ve ağ sağlamak için bazı altyapı planlamaları bağlantı. Ek olarak, işletim sistemleri ve kullanıcı yönetimi görevleri daha zor hale geldi ve desteklemesi için bir operasyon personeli gerektirdi. Ancak, bu sistemler artık bilgisayar odalarındaki uzman kadrolar onları desteklemekte. Baskı işlemleri çoğunlukla ortadan kalktı, Veriler masaüstünde görüntülenir veya basılı kopya için yerel bir yazıcıya gönderilir. Çoğu durumda, bilgisayar merkezleri hala büyük ana bilgisayarları desteklemektedir, ancak çok daha az yer kaplarlar eski makinelerden daha. Bu tesislerin bazıları LAN'ları desteklemek için dönüştürülmüş ve UNIX tabanlı sistemleri dağıtmıştır. Bununla birlikte, erişim kontrolleri, çevre korumaları ve yedek destek altyapısı Kararlılık, güvenlik ve kullanılabilirlik sağlamak için hala yerinde olmalısınız. Güvenlik uygulayıcısı Fiziksel güvenlik önlemlerinin yerinde ve etkili olduğunu.Daha önce belirtildiği gibi, bilgi işlem merkezi genellikle diğer işletme fonksiyonlarını destekleyen bir tesisin bir parçasıdır. Çoğu durumda, bu tesis tüm işi desteklemektedir. Desteklemek için fiziksel güvenlik geliştirilmeli tüm tesis içinde bulunan hesaplama merkezi için özel hususlarla birlikte. Aslında, koruyucu Tüm tesis içinde ve çevresinde uygulanan önlemler, bilgisayar için ek koruma sağlar merkezi.

# 

# 9.KORUYUCU ÖNLEMLER

Bilgi işlem tesislerine girişler, kritik bilgi işlem kaynaklarını korumak için kontrol edilmelidir. Masaüstü bilgisayarlar, yerel olarak depolanan değerli bilgilerle genellikle bir gece boyunca kalır. Bazı durumlarda, bu sistemler hassas sistemlerde oturum açmış durumdadır. Hassas verileri olan dizüstü bilgisayarlar gece ve hatta çalışma saatleri sırasında çalınabilir. Değerli bilgi kaynaklarını, insanları ve sistemleri korumak için çeşitli yöntemler ve araçlar göz önünde bulundurulmalıdır.

Katmanlı bir savunma, bir miktar fazlalık sağlayarak ve genişleterek erişim kontrollerine duyulan güveni arttırır.

Katmanlı bir savunmayı planlayan BT güvenlik uzmanı, üç temel ilkeye ayırır: genişlik, derinlik ve caydırıcılık.

Genişlik kullanılır, çünkü tek bir kontrol türü nadiren açıklıkların hepsini ortadan kaldırır. Örneğin; oturum açma şifresi kullanarak verilere okuma erişimini kontrol etmeye karar verdiğimizi varsayalım. Ancak, veriler İnternet üzerinden gönderilirse, oturum açma şifresi korunmaz. Bu nedenle farklı bir kontrol türü (yani şifreleme) ihtiyaç duyulur. Bu da genişliği temsil eder.

# 10.ÇEVRESEL ENDİŞELER

Çoğumuz, tesislerimizin nereye yerleştirileceğini belirleme fırsatımız yok çünkü muhtemelen Bilgi güvenliği görevlisi olarak atanmamızdan önce vardı. Ancak, bu bizi engellemez Hangi çevresel risklerin mevcut olduğunu belirlemeye çalışmak ve bunları azaltmak için harekete geçmek. Şanslıysanız tesislerin havayolları gibi tehditlere maruz kalma riskinin azaldığı alanlara taşınmasıyla ilgili girdilere sahip olması, deprem hataları ve taşkınlar.

## 10.1.Topluluk

Çevredeki topluluk, bilgisayar odası güvenliğine ve risklere katkıda bulunabilir. Sahip olan topluluklar Güçlü polis ve itfaiye hizmetleri tehdit ve olaylara hızlı bir şekilde cevap verebilecek. Düşük suç oranları AU1997\_Frame\_ch160 Sayfa 1948 14 Kasım 2003 Cuma 12:55 Hesaplama Tesisi Fiziksel Güvenlik 1949 ve güçlü ekonomik faktörler, bilgi işlem tesisleri için güvenliğin yanı sıra en iyi çalışanları cezbetmek. İdeal topluluk bulmak zordur ve çoğu durumda seçme şansınız olmaz bir. Bu topluluktaki diğer işletmeler, patlayıcı işlemler, kimyasal kirleticiler ve gürültü kirliliği gibi tehlikeler sağlayabilir. Topluluk havaalanları, havaalanına yakın olan iniş ve kalkış uçuş yollarına sahip olabilir. tesisi. Suç oranlarının yüksek olması, bilgi işlem tesisini ve sakinlerini de tehdit edebilir. Koruyucu önlemler Bu riskleri hesaba katmak için geliştirilmeleri gerekebilir. Güvenlik pratisyeni, bir ilişki geliştirerek topluluk yeteneklerinin değerini artırabilir. yerel polis ve yangından korunma örgütleri. Bu kuruluşlarla iyi bir ilişki sadece Tesislerin güvenliğine katkıda bulunur, ancak aynı zamanda acil durumlarda personelin güvenliğinin anahtarı olacaktır. Acil durum tatbikatlarına katılmaları ve süreci eleştirmeleri için davet edilmelidirler. Yerel polis, tesisleri gezmeye ve tesislerin yerleşimini anlamaya davet edilmeli ve koruyucu önlemler yerinde. Aslında, mevcut durum için önerilen iyileştirmeler sağlamaları istenmelidir. kullandığın önlemler. Yerel bir koruma servisiniz varsa, bir çalışanlarının bulunması şarttır. yerel polis yetkilileriyle ilişki. İtfaiye, yangından korunma önlemlerini gözden geçirmekten ve iyileştirmeye yardımcı olmaktan mutluluk duyacaktır. onlar. Birçok durumda, yangın söndürücüler ve diğer yangın söndürme gibi şeyleri incelemek için ısrar edecekler sistemleri. İtfaiyenin tesis yerleşimini ve giriş noktalarını anlaması çok önemlidir. çıkış. Ayrıca, kullanılan yangın söndürme sistemlerini ve bunlar için kontrollerin yerini bilmelidirler. Sistemler

## 10.2.Doğanın Davranışları

Çoğu durumda, Tabiat Ana'nın ruh halini veya gazabının sonuçlarını kontrol edemeyiz. Ancak yapabilirizen muhtemel olaylara hazırlanın ve etkilerini azaltmaya çalışın. Deprem tehditleri ek gerektirebilirSunucuların ve çevresel aygıtların devrilme nedeniyle tahrip olmalarını önlemek için destekleme ve bağlama kayışları

düşüyor. Karter pompalarının kurulması ve yukarıdaki ekipmanların yerleştirilmesi ile taşma riskleri azaltılabilirzemin kat. Fırtına ve fırtınalardan kaynaklanan elektrik kesintileri, kesintisiz güç kaynağı (UPS) sistemleri ve tesislerin uygun şekilde topraklanması ile ele alınabilir.

Doğal afetlerin kilit noktası, çoğu durumda yok edilememeleridir. Çareler olmalı

Bir olayın meydana gelme ihtimaline ve buna uygun bir şekilde karşılık verilmesine ilişkin hükümler esas alınarak tasarlandı. Tümündedurumlarda, tesis içi depolama veya yedek sistemler ile veri yedeklemesi yapay veya doğal olarak hazırlanmalıdır.

afetler.

## 10.3.Diğer Dış Riskler

11 Eylül 2001’de meydana gelen olaylara kadar isyanlarla ilgili fiziksel güvenlik kaygıları, işyerişiddet ve yerel bozulmalar. Ülkede terör eylemleri fikri uzak ama mümkün görünüyordu. Dan beriO tarihte, terörizm sadece mümkün değil, aynı zamanda olasıdır. Tesisleri çimento kullanarak korumaya yönelik önlemler

engeller, park edilmeyen bölgeler ve güvenlikli erişim kapıları hem yönetim hem de

Personel. Bu önlemlerin getirdiği maliyet ve uygunsuzluk birdenbire daha kabul edilebilir.Tesislerimizin birçoğu teröristlerin hedef alanın dışında olduğu düşünülen bölgelerde bulunmaktadır.

Saldırı. Ancak, Oklahoma Şehri bombalaması düşük hedef bölgede gerçekleşti. Şarbon problemleriboşaltılması muhtemel pek çok olanak var. Biyo-terörizm veya nükleer santrallere saldırı riskleri şimdi gerçek ve mümkün olduğu düşünüldü ve hemen hemen her şehirde görülebilir. Alternatif site planlaması dikkate alınmalıdır

iş sürekliliği ve fiziksel güvenlik planlarında.

## 10.4.Tesis

Bilgi işlem ortamlarımızı destekleyen tesisler, çekirdek sağlamada kuruluş için kritik öneme sahiptir. Ticari hizmetler ve fonksiyonlar. Bugün, işletmelerini işletmek ve müşterilerine hizmet sağlamak için bilgisayar ve telekomünikasyon kaynaklarına güvenmeyen çok az sayıda kuruluş var. Bu gerektirir tesisin hem fiziksel hem de mantıksal yönleri üzerinde güvenlik. Aşağıdaki tartışmaBilgi işlem merkezinde kullanım için göz önünde bulundurulması gereken fiziksel koruyucu önlemler ve bu

onu kuşat.

## 10.5.Koruma Katmanları

Bu senaryoda internet tarafından başlamak gerekirse öncelikle dış güvenlik duvarı tarafından istenmeyen yöndeki trafik kesilecektir. Bilinen ataklara karşı koruma sağlayan IPS sistemleri ile hem internet tarafından hem de diğer ağlardangelecek trafik engellenebilmektedir. Bu önlemlere ek olarak yük dengeleyici ile erişilebilirlik artırılmakta web uygulama güvenlik duvarı ile de daha karmaşık web tehditlerine karşı koruma sağlanmaktadır. En son katman savunma olarak istemci IPS ve istemci güvenlik duvarı kullanılmıştır. Bulunduğu ağdan gelecek olası bir saldırı bahsedilen ağ cihazlardan geçmeyeceği tek savunma olarak istemci güvenlik ürünleri kalmaktadır. Uygulanan bu katmanlı yapı ile saldırıların gelebilecekleri tüm yerler ve nitelik olarak bilinen saldırıların birçoğu engellenebilecektir.

# 11. KAYNAKLAR

* [**https://www.burakeksi.com/iso-27001-bilgi-guvenliginde-fiziksel-ve-cevresel-guvenlik-1/**](https://www.burakeksi.com/iso-27001-bilgi-guvenliginde-fiziksel-ve-cevresel-guvenlik-1/)
* [**http://www.cagataycebi.com/security/fiziksel\_ve\_cevresel\_guvenlik.pdf**](http://www.cagataycebi.com/security/fiziksel_ve_cevresel_guvenlik.pdf)
* [**https://ieeexplore.ieee.org/abstract/document/6523805**](https://ieeexplore.ieee.org/abstract/document/6523805)
* [**https://ieeexplore.ieee.org/abstract/document/6141247**](https://ieeexplore.ieee.org/abstract/document/6141247)
* [**http://www.sgaguvenlik.com/hizmetlerimiz/guvenlik-teknolojileri/fiziki-guvenlik-ve-guvenlik-teknolojileri/**](http://www.sgaguvenlik.com/hizmetlerimiz/guvenlik-teknolojileri/fiziki-guvenlik-ve-guvenlik-teknolojileri/)
* [**https://www.guvenlikonline.com/makale/212/-erisim-kontrol-sistemleri-kullanmak-icin-7-onemli-neden.html**](https://www.guvenlikonline.com/makale/212/-erisim-kontrol-sistemleri-kullanmak-icin-7-onemli-neden.html)
* [**https://www.guvenliweb.org.tr/dosya/sds57.pdf**](https://www.guvenliweb.org.tr/dosya/sds57.pdf)
* [**http://www.udhb.gov.tr/images/hizlierisim/efcecbe1f21e9fe.pdf**](http://www.udhb.gov.tr/images/hizlierisim/efcecbe1f21e9fe.pdf)
* [**https://bilgiguvenligi.saglik.gov.tr/files/BilgiG%C3%BCvenli%C4%9FiPolitikalar%C4%B1K%C4%B1lavuzu.pdf**](https://bilgiguvenligi.saglik.gov.tr/files/BilgiG%C3%BCvenli%C4%9FiPolitikalar%C4%B1K%C4%B1lavuzu.pdf)
* **Information Security Management Handbook**