

**ATATÜRK ÜNİVERSİTESİ**

**MÜHENDİSLİK FAKÜLTESİ**

**BİLGİSAYAR MÜHENDİSLİĞİ**

**Bilgisayar Bilgi Güvenliği ve Yönetimi**

**FİZİKSEL GÜVENLİK**

**Prof.Dr. A.Samet HAŞILOĞLU**

**Proje Yürütücüsü**

**150707027-SENANUR AYDIN**

**İÇİNDEKİLER**

[**1. GİRİŞ 4**](#_Toc7996866)

[**2. FİZİKSEL GÜVENLİK 4**](#_Toc7996867)

[**2.1 KISA BİR TARİHÇE 5**](#_Toc7996868)

[**2.2 ODAK DİKKATİNE NEREDE? 5**](#_Toc7996869)

[**2.3 Doğal Felaketler ve Kontroller 6**](#_Toc7996870)

[**3. İNSAN FAKTÖRÜ 7**](#_Toc7996871)

[**3.1 KİLİTLER 7**](#_Toc7996872)

[**3.2 JETON 8**](#_Toc7996873)

[**3.2.1 Mücadele-Tepki Jetonları 8**](#_Toc7996874)

[**3.2.2 Salak Kartlar 8**](#_Toc7996875)

[**3.2.3 Akıllı kartlar 8**](#_Toc7996876)

[**4. Erişim Kartı Türleri 9**](#_Toc7996877)

[**5. Biyometrik Cihazlar 9**](#_Toc7996878)

[**5.1 Parmak izi tarama 10**](#_Toc7996879)

[**5.2 Retina Taraması 10**](#_Toc7996880)

[**5.3 El Geometrisi 10**](#_Toc7996881)

[**5.4 Yüz tanıma 11**](#_Toc7996882)

[**6. TEST YAPMAK 11**](#_Toc7996883)

[**7. ÖZET 11**](#_Toc7996884)

[**8. Fiziksel güvenlik: Sonrası Tehdit 11 Eylül 2001 12**](#_Toc7996885)

[**8.1 Amerika neden bir hedef? 13**](#_Toc7996886)

[**8.2 Neden Endişe Edilmeli? 13**](#_Toc7996887)

[**8.3 Kurumunuz Potansiyel Bir Hedef midir? 14**](#_Toc7996888)

[**9. Terörist Amaçlara Örnekler 14**](#_Toc7996889)

[**10. Devlet kurumları 15**](#_Toc7996890)

[**11. Paradigma Değişimi: Önleme Önleme 16**](#_Toc7996891)

[**12. Terörizm Riskini Azaltma 17**](#_Toc7996892)

[**12.1 Fiziksel Güvenlik Değerlendirmeleri 18**](#_Toc7996893)

[**13. Terörizm Olayı Prosedürleri Oluşturma 23**](#_Toc7996894)

[**13.1 Bina Güvenliği Prosedürleri 25**](#_Toc7996895)

[**14. 11 Eylül'den Alınan Dersler 26**](#_Toc7996896)

[**15. İş Sürekliliği Planları 27**](#_Toc7996897)

[**16. Fiziksel Güvenlik Önlemleri 27**](#_Toc7996898)

[**17. Şüpheli Patlayıcı Bir Aygıtın Keşfi 30**](#_Toc7996899)

[**17.1 Tahliye 32**](#_Toc7996900)

[**18. Genel Güvenlik Prosedürleri 32**](#_Toc7996901)

[**19. Kurtarma 38**](#_Toc7996902)

[**19.1 Normal İşlemlere Devam Etme 39**](#_Toc7996903)

[**20. Dersler öğrenildi 39**](#_Toc7996904)

[**20.1 Önümüzdeki Çalışma 40**](#_Toc7996905)

[**21. Sonuç 40**](#_Toc7996906)

[**22. Kaynakça 41**](#_Toc7996907)

# 

# 1. Giriş

Bu bölüm, temel bilgisayar güvenliğinin iki temel unsurunu incelemektedir:

Fiziksel güvenlik ve Biyometri. Fiziksel güvenlik, kuruluşunuzun fiziksel bilgisayar tesislerini korur. Binaya, bilgisayar odalarına, bilgisayarlara (ana bilgisayar, mini ve mikro), manyetik ortama ve diğer ortamlara erişimi içerir. Biyometri cihazları fiziksel özellikleri (yani parmak izi, avuç içi baskısı, yüz özellikleri vb.) veya davranış özelliklerini (imza, yazma alışkanlıkları vb.) kaydeder [1,2].

# 2. FİZİKSEL GÜVENLİK

Herhangi bir kontrolün işyerine uygulanabilmesi için mevcut güvenlik seviyesinin değerlendirilmesi gerekir. Bu, birkaç yolla gerçekleştirilebilir. En kolay olanı “dolaşmak” tır. Mesai saatlerinden sonra tesisten yürüyüp beş kilit kontrolü kontrol edin:

1. Ofis kapıları kilitlendi.

2. Masalar ve dolaplar kilitlendi.

3. İş istasyonları güvende.

4. Disketler güvende.

5. Şirket bilgileri güvence altına alınmıştır.

Bu beş kilit kontrol elemanının kontrol edilmesi, halihazırda bulunan kontrol seviyelerinin temel bir şekilde anlaşılmasını ve bir güvenlik kontrol sistemi uygulandığında iyileştirmelerin ölçülmesinde bir ölçüt sağlayacaktır.

Tipik olarak, bu gözden geçirme neredeyse% 90 oranında bir kontrol eksikliği oranı gösterecektir. Yeni güvenlik kontrolleri yapıldıktan altı ila dokuz ay sonra ikinci bir inceleme yapılması önerilir.

# 2. KISA BİR TARİHÇE

Bilgisayar çağının başında, sistemleri korumak kolaydı; Laboratuarda kilitli kaldılar ve sadece birkaç seçilmiş “büyücüye” erişim sağlandı. Günümüzde bilgisayarlar daha ucuz, daha küçük ve neredeyse herkes için daha erişilebilir durumda.

Yirminci yüzyılın ortalarında, anabilgisayar için dünya çapında pazar bilgisayar sistemleri patladı. Üçüncü nesil sistemler 1960'larda mevcut olan şirketler, bu sistemlere bağımlılıklarını anlamaya başladı. 1970'lerin ortalarından sonuna kadar, güvenlik endüstrisi yetişmeye başladı: Halon yangın söndürme sistemleri, kart erişimi ve RACF ve ACF2. Yüzyılın son çeyreğinde ana bilgisayar merkezli bilgi işlem doruktaydı.

1983'te, uygun fiyatlı taşınabilir bilgisayar, bilgi güvenliği uzmanları için çalışma alanını değiştirmeye başladı. Ana bilgisayardan masaüstüne bir göç başladı. Geçtiğimiz yirmi yılda bu kadar zor kazanılmış olan kontroller artık bürokrasinin nedeni olarak kabul edildi [1].

Artık masaüstlerinde fiziksel güvenlik gerekiyor. Yıllar boyunca, geleneksel düşünce bir bilgisayarın bir bilgisayar olduğu yönündedir.

Denetimler, masaüstü veya iş istasyonu ortamında ana bilgisayar ortamından daha önemlidir.

Bilgi işlem ortamı şimdi masaüstünden kullanıcıya geçiyor.

Telekomünikasyonun kabul edilmesiyle, bir sonraki zorluk kullanıcı merkezli bilgi işlem ortamına fiziksel güvenlik çözümleri uygulamak olacaktır.

Her masadaki bilgisayarlar ağlarla diğer yerel ağlara bağlıyken ve uzak sistemlerde, fiziksel güvenlik ihtiyaçları gözden geçirilmeli ve gerekli olan yerde yükseltildi. Bilgisayar ve iletişim güvenliğindeki gelişmeler yeterli değildir; Fiziksel güvenlik, genel bir bilgi güvenliği planının hayati öneme sahip bir bileşeni olmaya devam etmektedir [3].

## ODAK DİKKATİNE NEREDE?

Herhangi bir fiziksel güvenlik uygulaması yapılmadan önce, bilgisayar sistemlerine yönelik mevcut tehditlere odaklanmak ve kaynakların en iyi harcanabileceği yeri belirlemek için sınırlı bir ticari etki analizi (BIA) yapmak yararlı olabilir. Tüm olası tehditleri, muhtemel olmayanları bile dikkate almak çok önemlidir. Phoenix'deki bir tsunami veya Maui'deki bir kum fırtınası gibi sıfır olma ihtimali olanları görmezden gelin. Çok basit bir BİA gösterildiği gibi çizilebilir. Sınırsız sayıda tehdit kuruluşunuz için endişe verici olabilir.

Herhangi bir sayıda yüksek olasılık tehdidi tespit edilebilir. Öncelikle, kuruluşunuzu gerçekten etkileyebilecek tehditleri (örneğin yangın, sel veya sahtekarlık) göz önünde bulundurun. Üç unsur genellikle her tehditle ilişkilendirilir:

• Madde: yıkıcı madde bir insan, bir makine veya doğa olabilir.

• Sebep: Yanlışlıkla ve kasten tehdit edebilecek tek ajan insandır.

• Sonuçlar: Bilgi sistemleri topluluğu için bu erişim kaybı veya yetkisiz erişim, değişiklik veya verilerin veya bilgilerin ifşası veya imhası.

Not: Her bir efekti 4 = yüksek - 1 = düşük olarak sıralayın. Her bir kaynağı 4 = zayıf kaynak, 1 = mevcut güçlü kaynak temelinde sıralayın.

Fiziksel güvenliğin odağı genellikle sabotaj, hackleme ve insan hatası gibi insan kaynaklı felaketler olmuştur. Aynı tür tehditlerin doğal afetlerden de kaynaklanabileceğini unutmayın.

## Doğal Felaketler ve Kontroller

Yangın - Bir çakışma, bilgi sistemlerini ısı, duman ya da bastırma ajanı (örneğin, yangın söndürücüler ve su) hasarlarından etkiler. Bu tehdit kategorisi küçük, büyük veya yıkıcı olabilir. Kontroller: ekipmanın yanına duman dedektörleri takın; Yangın söndürücüleri ekipmanın yakınında bulundurun ve çalışanları uygun kullanımları için eğitin; Düzenli yangın tahliye tatbikatları yapar.

Çevresel başarısızlık - Bu felaket türü, ülkeye sağlanan kontrollü çevre desteğinin temininde herhangi bir kesinti içermez.

operasyon merkezi. Çevresel kontroller temiz hava, klima, nem ve su içerir. Kontroller: insanlar ve bilgisayarlar iyi bir arada bulunmadığından, onları ayrı tutmaya çalışın. Birçok şirket çalışanlar için komuta merkezleri ve makineler için “ışıklı” bir ortam kuruyor. Bilgisayar içeren tüm odaları makul sıcaklıklarda tutun (60 - 75 ° F veya 10 - 25 ° C). Nem seviyelerini% 20 ila 70 arasında tutun ve çevre ayarlarını izleyin [6].

Deprem - Şiddetli bir yer hareketi, yeryüzündeki stres ve hareketlerden kaynaklanır. Kontroller: bilgisayar sistemlerini cam ve yüksek yüzeylerden uzak tutun; yüksek riskli bölgelerde bilgisayarları antivibrasyon cihazlarıyla sabitleyin.

**Örnek 1. İş Etki Analizi Örneği.**

Sıvı Sızıntısı - Bir sıvı sızıntısı patlama veya sızıntı yapan boruları içerir.

ve fıskiyelerin yanlışlıkla boşaltılması. Kontroller: sıvı geçirmez kapakları ekipmanın yakınında tutun ve bilgisayar sistemlerinin yakınındaki yapısal zemine su dedektörleri takın.

Yıldırım - Bir elektrik yükü, tesise doğrudan yıldırım çarpması veya elektrik enerjisi iletim hatlarına, trafolara ve trafo merkezlerine yapılan grev nedeniyle dalgalanmalara neden olabilir.

Kontroller: aşırı gerilim koruyucuları kurun, yedekleri topraklanmış depolama ortamına koyun, Kesintisiz Güç Kaynağı (UPS) ve dizel jeneratörleri kurun ve test edin.

Elektrik Kesilmesi - Elektrik beslemesinde kesinti,

genellikle bir buçuk saatten uzun süren, ciddi bir iş etkisi olabilir.

Kontroller: UPS'i kurun ve test edin, voltaj yükselmelerini kontrol etmek için hat filtreleri takın ve antistatik halılar takın.

# 3. İNSAN FAKTÖRÜ

Son FBI istatistikleri, tüm hırsızlık, sahtekarlık, sabotaj ve kazaların% 72'sinin bir şirketin kendi çalışanlarından kaynaklandığını göstermektedir. % 15 ila 20 oranında başka bir bina, sistem ve bilgiye erişim sağlayan müteahhit ve danışmanlardan geliyor. Sadece% 5 ila 8'i dış insanlar tarafından yapılıyor, ancak basın ve yönetim çoğunlukla bunlara odaklanıyor. Tipik bilgisayar suçlusu, kontrol eksikliklerini tespit etmek için yeterince uzun süredir devam eden, teknik olmayan, yetkili bir kullanıcıdır.

Kontrol cihazlarını uygularken kontrollerin yapıldığından emin olun.

kuruluşun gereksinimlerini karşılayın. Dahili erişimin bir incelemesini dahil edin ve çalışanların dış kaynaklara uygulanan özen standartlarını karşıladığından emin olun. “Davetsiz misafir” bir binaya, sisteme veya verilere girme yetkisi olmayan herhangi birini içerebilir.

İşgalcilere karşı ilk savunma onları binadan veya bilgisayar odasından uzak tutmak. Bununla birlikte, son yirmi yıldaki maliyet azaltıcı önlemler nedeniyle, artık çok az bilgisayar tesisi korunmaktadır. Her yerde bilgisayarlarla, kilitlerin nereye takılacağını belirlemek önemli bir sorundur.

Herhangi bir iş ortamına erişmek için herkes bir kimlik doğrulama ve / veya yetkilendirme testinden geçmek zorundadır. Kullanıcıları doğrulamanın üç yolu bir şey içerir:

• Kullanıcının bildiği bir şifre (şifre).

• Kullanıcının sahip olduğu (bir rozet, anahtar, kart veya jeton).

• Fizyolojileri arasında (parmak izi, retina görüntüsü, ses).

## KİLİTLER

Kampüsü güvenceye almanın yanı sıra, bilgisayarlar, ağlar, disk sürücüleri ve elektronik ortamlar. Bir iş istasyonunu sabitlemenin bir yöntemi, bir iş istasyonu yüzeyine tutturulmuş kilitleme çubuklarına sahip metal bir ped olan bir bağlantı pedidir. Mekanizma bilgisayarın kabuğuna kurulur. Bunlar birçok satıcıdan temin edilebilir.

Birçok kurum kablo ve kilit kullanır. Güvenlik kabloları, güvenlik kablosunu masaya veya başka bir düzeneğe sabitleyen, sabit bir şekilde tutturulmuş bir plaka ile iş istasyonuna yapıştırılmış uçak tipi çelik kablolardır.

Disk kilitleri, iş istasyonunu güvence altına almanın başka bir yoludur. Bunlar küçük cihazlar hızlı bir şekilde disket yuvasına yerleştirilir ve ünitedeki diğer tüm disketleri kilitler. Yetkisiz önyüklemenin disketten ve virüslerden kaynaklanan enfeksiyonlardan korunmasını önleyebilirler.

Kriptografik kilitler ayrıca görüntüleyerek yetkisiz erişimi önler yetkisiz personele okunamayan bilgiler. Şifreleme yazılımı, hassas işletme bilgilerinin gizliliğini sağlarken günlük işlemleri etkilemez. Kriyografik kilitler uygun maliyetlidir ve kolayca temin edilebilir.

## JETON

İnsan güvenliği güçleri küçüldükçe, yalnızca yetkili personelin bilgisayar odasına girebilmesini sağlamak için daha fazla ihtiyaç vardır. Belirteç, kullanıcının kimliğini doğrulamak için taşıdığı nesnedir. Bu aygıtlar kartlı kartlar, kart okuyucular veya biyometrik aygıtlar olabilir. Aynı amaca sahipler: kullanıcıyı sisteme doğrulamak. En yaygın biçim, normalde taşımaya yetkili kişi hakkında kodlanmış bilgiler içeren elektrikli bir cihaz olan karttır. Belirteçler tipik olarak başka bir kimlik doğrulama türü ile kullanılır. Birçok şifre kilitleri token card access sistemleri ile değiştirildi.

### 3.2.1 Mücadele-Tepki Jetonları

Mücadele yanıtı belirteçleri, kimlik doğrulama isteyen işlemlerden (Güvenlik Dinamikleri’nin SecurID’si gibi) bir sorun kullanılarak oluşturulan şifreleri sağlar. Kullanıcılar kendilerine tahsis edilmiş kullanıcı kimliklerini ve şifrelerini ve ayrıca belirteç kartı tarafından sağlanan şifreyi girerler. Bu işlem, kullanıcının sahip olduğu bir şeyi (belirteç) ve bildiği bir şeyi (mücadele / yanıt süreci) tedarik etmesini gerektirir. Bu işlem parola koklama ve kaba kuvvet saldırılarını boşuna harcar. Challenge-cevap asenkron bir süreçtir. Meydan okumaya bir alternatif, sistemden bir meydan okuma girilmeden şifreyi oluşturan senkronize belirteçtir. Kullanıcı ve belirteç kombinasyonu sisteme kaydedildiğinde kimlik doğrulaması yapan bilgisayarla senkronize edilir.

### 3.2.2 Salak Kartlar

Uzun yıllardır çoğu insan için fotoğraflı kimlik kartı kimlik belgesi niteliğindedir. Sürücü ehliyetleri, pasaportları ve çalışan kimliği rozetleri ile, resim - kişinin istatistikleriyle birlikte - kimlik doğrulama işleminin tamamlanması için yeterli bilgi sağlar. Çoğu kişi rozeti güvenlik görevlisine vurur veya banka memuruna lisans verir. Birisi görsel olarak kimlik sahibinin yüzünü karttaki bilgilerle eşleştirir.

### 3.2.3 Akıllı kartlar

Otomatik vezne makinesi (ATM) kartı

“Aptal kart”; bu “akıllı” kartlar, kullanıcının erişim sağlamak için kartla birlikte kişisel bir kimlik numarası (PIN) girmesini gerektirir. ATM, manyetik şeritte kodlanan bilgileri, ATM makinesine girilen bilgiler ile karşılaştırır.

Akıllı kart, bir işlemci, programları ve verileri depolamak için kullanılan belleği ve bir tür kullanıcı arayüzünü içeren mikroçipler içerir. Hassas bilgiler, hafızasında, üretim sırasında kodlanan ve kart sahibinin erişemeyeceği gizli bir salt okunur alanda tutulur.

Genellikle, bu kartlar bilgileri koruyan bir tür şifreleme yöntemi kullanır. Tüm akıllı kartlar kart okuyucularla çalışmaz. Bir kullanıcı kartı okuyucuya yerleştirir, sistem bir mesaj görüntüler ve eğer bir eşleşme varsa, kullanıcıya erişim verilir.

# 4. Erişim Kartı Türleri

Erişim kartları, orijinalliği sağlamak için farklı teknolojiler kullanır:

• Fotoğraflı kimlik kartları, kullanıcının yüzünün bir fotoğrafını içerir ve görsel olarak kontrol edilir.

• Optik kodlu kartlar, ikili sıfırları ve bireyin kodlanmış kimlik numarasını içerenleri temsil eden küçük, fotoğrafla kazınmış veya lazer yanmış noktalar içerir. Kartın koruyucu laminasyonu, verileri yok etmeden ve kartı geçersiz kılmadan çıkarılamaz.

• Elektrik devre kartlarında basılı devre deseni bulunur. Bir okuyucuya yerleştirildiğinde, kart bazı elektrik devrelerini kapatır.

• En yaygın kullanılan erişim kontrol kartı biçimi olan manyetik kartlar, kodlanmış halde kullanıcının kalıcı kimlik numarasını içeren manyetik parçacıklar içerir. Veriler kartta kodlanabilir, ancak bandın kendisi değiştirilemez veya kopyalanamaz.

• Metalik şeritli kartlarda bakır şerit sıraları var. Striplerin varlığı veya yokluğu kodu belirler.

# 5. Biyometrik Cihazlar

Her insan, incelenip ölçülebilen benzersiz fizyolojik, davranışsal ve morfolojik özelliklere sahiptir. Biyometri, bu özelliklerin olumlu kişisel kimlik tespiti için kullanılmasıdır. Parmak izleri ve imzalar, bir kişinin kimliğini kanıtlamak için yıllarca kullanılmıştır, ancak bireyler başka birçok şekilde tanımlanabilir. Bilgisayarlı biyometri tanımlama sistemleri belirli bir özelliği inceler ve bu bilgileri kullanıcının bir binaya girip giremeyeceğini, bilgisayarın kilidini açıp açamayacağını veya sistem bilgilerine erişip erişemeyeceğini belirlemek için kullanır.

Biyometrik cihazlar, bireye özgü bilgileri toplamak için video kamera, retinal tarayıcı veya mikrofon gibi bir tür veri giriş cihazı kullanır. Kimlik doğrulama işleminde bir kullanıcının biyometrik karakteristiğinin (parmak izi, ses vb.) Sayısallaştırılmış bir gösterimi kullanılır. Bu kimlik doğrulama türü neredeyse sahtekarlığa karşı korumalıdır ve asla yanlış yerleştirilmez. Veriler nispeten statiktir ancak mutlaka gizli değildir. Bu kimlik doğrulama işleminin avantajı, giriş cihazlarına doğru verileri sağlamasıdır.

## 5.1 Parmak izi tarama

Birey, parmağını tarayan, parmak izini sayısallaştıran ve dosyada depolanan bir parmak izi görüntüsüyle karşılaştıran bir okuyucunun içine ya da parmağını yerleştirir. Bu yöntem, kişilerin kimliklerini doğrulamak veya bilgileri tanımak için birçok kişiyi kapsayan bir veri tabanıyla karşılaştırmak için kullanılabilir. Performansı:

• Yanlış reddetme oranı =% 9,4

• Yanlış kabul oranı = 0

• Ortalama işlem süresi = 7 saniye

## 5.2 Retina Taraması

Bu cihaz, kullanıcının lazerin kan damarlarının desenini taradığı bir merceğe bakmasını gerektirir. Desenler pozitif tanımlama sağlamak için karşılaştırılır. Bu yaklaşık 2,650 dolar.

Performansı:

• Yanlış ret oranı =% 1.5

• Yanlış kabul oranı =% 1.5

• Ortalama işlem süresi = 7 saniye

## 5.3 Avuç İçi Taraması

Sistem, insan avucunun 2 inç karelik bir alanından 10,000 nokta bilgi tarar. Bilgiyle, sistem kişiyi sahtekâr veya sahtekar olarak tanımlar. Tipik fiyat 2,500 dolar. Performansı:

• Yanlış reddetme oranı = 0

• Yanlış kabul oranı =% 0.00025

• Ortalama işlem süresi = 2-3 saniye

## 5.4 El Geometrisi

Bu cihaz tanımlama sağlamak için üç boyutlu el geometrisi ölçümlerini kullanır. Tipik fiyat 2.150 dolar. Performansı:

• Yanlış ret oranı =% 0.1

• Yanlış kabul oranı =% 0,1

• Ortalama işlem süresi = 2 ila 3 saniye

## 5.5 Yüz tanıma

Doğrulama yerine monte edilmiş bir kamera kullanarak (kapı, monitör vb.), Cihaz giriş yapan kişinin görüntüsünü, sisteme endeksli yetkili kullanıcının kayıtlı görüntüsü ile karşılaştırır. Tipik fiyat 2,500 dolar.

Performansı:

• Ortalama işlem süresi = 2 saniye

## 5.6 Ses Doğrulama

Bir kişi belirli bir cümleyi bir mikrofona konuştuğunda, bu cihaz ses düzenini analiz eder ve depolanan bir veri tabanıyla karşılaştırır. Fiyat, 3.000 kullanıcı için 12.000 $ 'a kadar çıkabiliyor. Performansı:

• Yanlış reddetme oranı =% 8,2

• Yanlış kabul oranı =% 0,4

• Ortalama işlem süresi = 2 - 3 saniye (cevap süresi şifre veya cümlenin gerçekten ses doğrulama sistemine konuşmasından sonra hesaplanır).

# 6. TEST YAPMAK

Güvenlik sistemleri, şifreler, kilitler, kartlar, biyometri ve diğer kimlik doğrulama cihazlarının kurulu olduklarından itibaren doğru şekilde çalışması beklenir, ancak bunların çalışmasını sağlayan yönetim ve testtir. Çalışanlar acil yangın çıkışlarını rutin olarak kullanıyorlarsa, bilgisayar odası için ayrıntılı bir erişim kontrol sistemi kurulmasında çok az nokta vardır. Çalışanlar, fiziksel güvenlik sistemlerinin doğru kullanımı konusunda eğitilmelidir. Erişim günlükleri zamanında izlenmeli ve uzlaştırılmalıdır.

Eğitim ve farkındalık zaman, para ve personel gerektirir, ancak kuruluşların artan rekabet ve azalan kaynaklar nedeniyle ortaya çıkan zorlukların üstesinden gelmesi esastır. Teknoloji ve çalışanlar arasında bir ortaklık olmalı. Teknolojiyi tedarik etme ve kurma gibi çalışanların eğitimi için en az zaman harcamak ve kaynak harcamak. Çalışanlar, kontrol mekanizmalarının neden seçildiğini ve güvenlik sürecinde rollerinin ne olduğunu anlamalıdır.

# 7. ÖZET

Çalışanların başkalarının içinden geçebileceği kapıyı açtığı şirketlerin güvenlik farkındalık düzeylerini gözden geçirmeleri gerekebilir. Fiziksel güvenlik programının uygulanmasındaki ilk adım, ihtiyaç seviyesinin ve mevcut farkındalık seviyesinin belirlenmesidir. Uygun maliyetli bir güvenlik programı uygulamak (1) sorunları analiz etmek, (2) kontrolleri tasarlamak veya tedarik etmek, (3) bu kontrolleri uygulamak, (4) bu kontrolleri test etmek ve uygulamak ve (5) kontrolleri izlemek. Yalnızca mevcut ihtiyaçları karşılamak için gereken kontrolleri uygulayın, ancak gerekirse daha sonra ilave kontrollerin eklenebileceğinden emin olun. Fiziksel güvenlik bir kuruluşun hırsızlığa, sabotajlara ve doğal afetlere karşı ilk savunma hattıdır.

# 8. Fiziksel güvenlik: 11 Eylül 2001 Sonrası Tehdit

Her şeyi değiştiren gün benim için sabah saat 5: 50'de başladı. Uyandım ve televizyonda bazı haberleri izlemeye başladım. Bu, 11 Eylül 2001, Salı sabahıydı. Yerel haber istasyonum

Sadece düzenli yayınını kesintiye uğratıp CNN’e geçti, o yüzden hemen önemli bir şey olduğunu biliyordum. Bir uçağın New York'taki Dünya Ticaret Merkezi kulelerinden birine çarptığını öğrendim. Güvensizlikle mutfağa giderken kendime bir fincan kahve döktüm. Televizyona döndüm ve gazetecileri dinledim ve havayolu uzmanları bu olayın olası nedenini tartışıyorlar [4].

Kendi kendime düşündüm, “gökyüzünde bir bulut yok; Bir uçak yanlışlıkla bu kadar büyük bir yapıya nasıl çarpabilir? ”

Bilmek, ama cevabı kabul etmek istememekle, televizyonun daha iyi bir sonuç vereceğini umarak dinledim.

Asla gelmeyen cevabı beklerken, ekranın sağ tarafından bir uçak geldiğini fark ettim. Ticaret Merkezi'nin kulelerinin arkasına gidiyor gibiydi, ya da belki de sadece olacağını umuyordum. Bu, zamanın dramatik bir şekilde yavaşladığı göründüğü örneklerden biriydi. Bölünmüş saniyede uçağın kulelerin arkasından çoktan çıkmış olması gerektiğinin farkına varıldı, ateş topu bunun yerine kulenin dışına fırladı. Şimdi inkar edilemezdi. Bu bir kaza değildi. Daha sonra başka bir fincan kahve içtikten sonra, sadece sigara görmek için televizyona geri döndüm; Sadece bir binanın yeni inşaat için yol açmaya başladığında gördüğünüz duman türü. Korkum için bir kulenin yıkıldığını biliyordum. Ardından, gazeteciler şoktan kurtulurken ve havadaki uyuşmalarını korumaya çalışırken, kalan kulenin tepesini gösterdiler. Bazı nedenlerden dolayı, kameranın yukarı kaydırmaya başladığı anlaşıldı. Biraz baş dönmesi hissetmeye başladım. Sonra, bir kez daha korkunç bir aydınlanma gerçekleşti. Kamera açılmıyordu; bina yıkılıyordu.

Dakikalar içinde, Dünya Ticaret Merkezi artık yoktu; ve Manhattan duman tarafından tamamen gizlendi. Tamamen güvensizlik içindeydim. Bu bir film olmalıydı; Ama değil. Zihnin kendini savunması, bir şey yapamadığı zaman meydana geldiğinde üstlenir ve kendimi tamamen uyuşmuş hissettim. Canlı TV'de anlatılmamış binlerce insanın ölümüne şahit oldum. 3000 mil uzakta olsam da, sahip olabileceği gibi

caddede oldu. Etki aynıydı. Ardından Pentagon'daki kazanın haberi geldi, ardından Pennsylvania'daki uçağın kazası.

Şu anda işler çok önemsiz görünse de işe gitmek için kendimi oluşturmaya çalıştım.

Her nasılsa kendimi bir araya getirip kapıdan çıktım. İşe giderken kendime bunun benim kuşağımın İnci Limanı olması gerektiğini düşündüm. Ve farkettim ki, ülkem muhtemelen savaştaydı - peki kiminle?

Birincisi, 11 Eylül sabahını hatırlamam. Bu gün, tarihte hepimizin nerede olduğumuzu ve ne yaptığımızı hatırladığımız o günlerden biri haline geldi. Hepimiz o korkunç günde kendi bireysel deneyimlerimiz olmasına rağmen, bazı insanlar diğerlerinden daha çok etkilenmiş olsa da, bu bireysel deneyimler hepimizi şaşırtan ve şok eden kolektif bir deneyim oluşturur.

Dünyanın her yerindeki ve özellikle ABD'deki güvenlik uygulayıcıları kendilerine bazı sorular sormak zorundadır. Bu burada olabilir mi? Kuruluşum potansiyel bir hedef mi? Şimdi 11 Eylül saldırılarının sonucunda Teröre Karşı Savaş başladığı için, bu soruların her ikisinin de cevabı ne yazık ki “evet”.

Ancak, riski azaltmak için yapılabilecek bazı şeyler var. Bu bölüm terörizm riskinin neden arttığını, ne tür kuruluş veya tesislerin daha yüksek risk altında olduğunu ve bu riski azaltmak için neler yapılabileceğini incelemektedir.

## 8.1 Amerika neden bir hedef?

ABD Hava Kuvvetleri Özel Harekat Merkezi'nden Terörist grupların Amerika’yı hedef almasının birçok nedeni var. Bunun bir nedeni ideolojik farklılıklar. Amerikalılar tarafından benimsenen özgürlük ve hoşgörüyü takdir etmeyen uluslar veya kültürler var. Amerika, tartışmasız dünyanın lider sanayi gücü ve kapitalist devletidir. Dünyada Amerika'yı bir soygun baronu olarak görebilecek ve algılanan zenginliğimizden dolayı Amerikalılardan nefret edebilecek insanlar var. Diğer bir sebep ise dini farklılıklar. Dini değerleri ve inançlarıyla uygunsuzluk algılanması nedeniyle Amerika ve Batı'yı hor görebilecek dini güdümlü gruplar var. Diğer bir neden, ABD hükümetinin diğer hükümetlerin eylemleri üzerinde çok fazla etkisi olduğu algısıdır. Teröristler, terör eylemleriyle ABD hükümetinin müzakere edeceğini ve nihayetinde taleplerine uyacağını düşünebilir. Ancak, hükümetimiz teröristler ile pazarlık yapmayacağını defalarca belirtti.

Nihai neden, Amerikalıların kolay hedefler olarak algılanmasıdır. Amerika’da ve birçok Batı ülkesinde “açık toplum” teröristlerin kolay hareket etmesini ve faaliyetlerini kolaylaştırıyor. İster hayır kurumlarında, işletmelerde, kamu kapasitelerinde, ister turist olarak performans olsun, Amerikalılar tüm dünyada. Bu, Amerikalıları hedef almayı göreceli olarak zayıf eğitimli terörist gruplar için bile oldukça kolaylaştırmaktadır. Tüm dünyaya yayılmış olan ABD askeri kuvvetleri, ABD gücünün görünür sembolleri olarak görülmektedir ve bu nedenle teröristlere de çekici hedefler getirmektedir.

## 8.2 Neden Endişe Edilmeli?

Terörizm, korkunun telkin edilmesi için hesaplanan şiddet kullanımı veya şiddet tehdidi olarak tanımlanabilir; genel olarak politik, dini veya ideolojik olan hedeflerin peşinde hükümetleri veya toplumları zorlamak veya bunlara göz yummak amacıyla tasarlanmıştır. Bazı terörist amaç ve taktik örnekleri Örnek 163.1'de görülebilir.

Terörizm ve siber terörizm tehdidindeki artış, bilgi güvenliği uygulayıcıları için yeni ve önemli bir husustur. Önceden, fiziksel güvenlik tehditleri yetkisiz erişim, suç, çevre koşulları, sert hava koşulları, depremler, vs. gibi şeyleri içermekteydi. 11 Eylül olayları bize tam olarak ne kadar savunmasız olduğumuzu gösterdi. Güvenlik uygulayıcılarının o günden alabilecekleri en önemli derslerden biri de terörizmi içerecek şekilde fiziksel güvenlik uygulamalarımızı yeniden değerlendirme ihtiyacını tanımaktır. Karışıma terörizm eklemek, geleneksel fiziksel güvenliği görme biçimimizde bazı temel değişiklikleri gerektiriyor. Bu değişikliklerin teröre karşı koruyucu tedbirler içermesi gerekiyor.

Örgütün türüne bağlı olarak, teröristlerin onu hedef alabilmesi oldukça olası. İster fiziksel yıkım için tesisleri veya ofisleri hedefler, isterse siber saldırı için bir organizasyon seçtiler, temkinli bilgi güvenliği uygulayıcıları hedef aldıklarını ve buna göre plan yaptıklarını varsayarlar.

## 8.3 Kurumunuz Potansiyel Bir Hedef midir?

Pek çok kuruluş teröristlerin potansiyel hedefi olabilir ve savunmasız olduklarını bile bilmiyorlar. Federal, eyalet ve yerel de dahil olmak üzere devlet kurumları ve altyapı şirketleri temel hedefler olabilir.

 Diğer savunmasız kuruluşlar, dünyadaki Amerikan ürünlerini pazarlayan çok uluslu şirketler ve tanınmış gökdelenlerde bulunan kuruluşlar olabilir. Bu tür potansiyel hedeflerin spesifik örnekleri, onları daha yüksek risk altına sokma ihtimalini önlemek için adlandırılmayacaktır. Farklı potansiyel hedef türleri için bkz. Sergi 163.2.

# 

# 9. Terörist Amaçlara Örnekler

Grubun davasının tanıtımını yapın

Grubun gücünü göster

Mevcut hükümetin güç eksikliğini göster

İntikam almak

Lojistik destek alın

Hükümetin aşırı tepki göstermesine neden olmak

Ortak Terörist Taktikleri

Suikast

Kundakçılık

bombalama

Rehine almak

kaçırma

Kaçırma veya skyjacking

haciz

Tesislere saldırılar veya saldırılar

Sabotaj

Aldatmacalar

Özel silah kullanımı

Çevresel tahribat

Teknoloji kullanımı

# 10. Devlet kurumları

ABD hükümetinden ve birçok Batı ülkesinden nefret eden birçok terörist var. Teröristlerin ve sempatizanların kafasında, hükümetler politikaları yaratıyor ve şiddetle karşı çıktığı değerleri temsil ediyorlar. Bir roket bilimcisi veya bu konuda bilgi güvenliği uygulayıcısı almaz,

ABD hükümetinin ajanslarının teröristler için ana hedef olduğunun farkına varmak. Bu, elbette, ABD ordusunu da içerir. Diğer Batı ülkeleri, özellikle ABD’yi Terörle Mücadelede destekleyenler, kendilerini teröristlerin hedefleri de bulabilirler. Eyalet ve yerel yönetimler de risk altında olabilir.

• Altyapı şirketleri. Altyapıyı oluşturan şirketler de artan terör riskiyle karşı karşıya. Teröristler yalnızca ABD’ye ve Batı hükümetlerine zarar vermek istemeyecek, aynı zamanda normal yaşamı ve Batı dünyasının ekonomilerini de bozmak isteyebileceklerdir. Enerji, seyahat, finans ve bilgi akışını bozmak bunu başarmanın bir yoludur. Tıp sektörü de burada yer almaktadır. İnsan şimdi daha önce düşünülemez olanı düşünmeli, her zamanki zihniyetlerimizin ötesine bakmalı ve tıbbi tesisler daha önce hedef alınmadığı için gelecekte hedeflenebilecekleri düşünülebilir.

• Lokasyon bazlı hedefler. Ayrıca, konumlarının veya işlevlerinin risk altında olduğu hedefleri de vardır. Tıpkı Dünya Ticaret Merkezi'nin kulelerinin Amerikan ekonomisinin 11 Eylül teröristlerine verdiği gücü temsil etmesi gibi, diğer yerler de düşmanca niyetli olanlara özgü olan Amerikalıları temsil ediyor olarak yorumlanabilir. Bu yerler, büyük şehirlerdeki gökdelenleri veya Amerikan veya Batı çıkarlarını temsil eden çeşitli simge yapılardan herhangi birini içerebilir. Popüler turist destinasyonları veya çok sayıda insanın katıldığı etkinlikler de riskli olabilir çünkü bunlar benzersiz bir şekilde Amerikan / Batı olmaları veya çok yoğun olmaları nedeniyledir.

• Amerika anlamına gelen şeyler. Dikkate alınması gereken başka bir kategori var. Bu kategori yukarıdaki kategorilerle biraz örtüşüyor, ancak yine de söz edilmeyi hak ediyor. Amerika'yı veya Batı'yı dünyanın geri kalanına temsil eden büyük şirketler de hedeflenebilir. Bu aynı zamanda ürünleri dünya çapında satılan ve Amerika'yı dünya insanlarına temsil eden şirketleri de içermektedir [5].

SERGİ 163.2 Potansiyel Terörist Hedefler

Devlet kurumları

ABD federal ajansları

ABD askeri tesisleri

Devlet hükümetleri

İlçe hükümetleri

Yerel yönetimler

altyapı

Enerji

taşımacılık

mali

Su

Internet

Tıbbi

Konum tabanlı

Uzun ofis binaları

Ulusal yerler

Popüler turistik yerler

Büyük olaylar

Amerika ile ilişkili

Batı dünyası ile eşanlamlı büyük şirketler

Amerikan veya ABD adına

Ünlü Amerikan marka ürünlerini üreten şirketler

Bir kuruluş yukarıdaki kategorilerden birine girerse, terörizmden daha önce düşünüldüğünden daha büyük bir risk ile karşı karşıya kalabilir. Bir kuruluş yukarıdaki kategorilerden birine uymuyorsa, bilgi güvenliği uygulamalarının mümkün olan en fazla anti-terörizm önlemi almaları tavsiye edilmektedir.

# 11. Paradigma Değişimi: Önleme Önleme

*İş, diğer mesleklerden çok, geleceğe yönelik sürekli bir iştir; bu sürekli bir hesaplamadır, öngörüde içgüdüsel bir alıştırmadır.*

- *Henry R. Luce*

Fiziksel güvenlik işletme paradigması caydırıcı olmuştur. Bir failin yakalanmak, tutuklanmak veya hatta öldürülmek istememesi fikri, kabul edildiğimizi düşündüğümüz şekilde kök saldı. Muhtemelen şimdiye kadar hepimizin bildiği gibi, hararetli dini inançlar ya da bu bakış açısını paylaşmayan politik sebepler tarafından motive edilmiş insanlar var; nedenlerini ileri süreceklerine inandıkları bir eylemde bulunmak için ölmeye istekli olabilirler hatta ölmek isteyebilirler.

Günümüzde endüstri standardı olarak kabul edilen çoğu güvenlik koruması, caydırıcılık paradigmasına dayanmaktadır. Kameralar, alarmlar, röntgen veya kızılötesi algılama gibi güvenlik cihazlarının tümü, yakalanmak istemeyen bir failin caydırılması amacıyla kullanılmaktadır. Her ne kadar caydırıcılığa dayalı tedbirler, fiziksel güvenlik tehditlerinin ezici çoğunluğu için yeterli güvenlik sağlayacak olsa da, bu önlemler bir terör eylemi gerçekleştirirken ölmeyi planlayan birine karşı büyük ölçüde etkisiz olabilir.

11 Eylül 2001 sabahı, acı verici bir ders öğrendik: caydırıcılık, aklındaki her türlü eylemi sürdürmek için ölmek isteyenleri caydırmaz. Ne yazık ki, bu fiziksel güvenliği çok daha zor ve pahalıdır. Bilgi güvenliği pratisyenlerinin yaygın kabul gördüğünün farkında olması gerekir

güvenlik kameralarına, şifreli kapılara ve kimlik kartlarına sahip olmak gibi standartlar yalnızca potansiyel bir teröristi yavaşlatabilir. Davetsiz misafirleri caydırmak için çalışmak yerine, şimdi daha önce düşünülmemiş olan - intihar teröristini de düşünmeliyiz. Bu, terörist bir eylemde bulunmak için ölmek isteyen birinin önlenmesi için ne gibi önlemler alınması gerektiği anlamına gelir.

Fiziksel Güvenlik: 11 Eylül 2001 1979’dan Sonra Tehdit

Havayolu endüstrisi, 11 Eylül’de gerçekleşen olayların tekrarlanmasını önlemek için çok daha sıkı güvenlik önlemlerinin gerekli olduğunu öğrenmiş gibi görünmektedir. Daha önce, bir havayolu şirketinin en kötü kabusu bir uçağın bombalanması ya da kaçırılmasının ardından rehin yolcularını serbest bırakmak için gergin görüşmeler yapmaktı. . Hiç kimse bir uçağı kitle imha silahı olarak kullanma tehdidini düşünmedi. O zamandan beri uçuşan herkes ek gecikmelere, aramalara ve kimlik kontrollerine aşinadır. Rahatsız edici ve gezgin yavaşlatmak; Ancak, daha iyi güvenlik için ödemek için küçük bir fiyattır.

Hala yapılacak daha çok iş olmasına rağmen, bu önleme paradigmasının kullanılmasına bir örnek teşkil ediyor.

Havayolları bu tür olayların önlenmesi için birçok güvenlik önlemi almıştır. Ne yazık ki, olduğu gibi

bilgi güvenliği, mutlak fiziksel güvenlik diye bir şey yoktur. Önceden düşünülmeyen bir şeyin ortaya çıkma olasılığı her zaman vardır. Bilgi güvenliği uygulayıcıları ayrıca gerekli fiziksel güvenlik değişikliklerini yapma yeteneklerini sınırlandırabilecek kurumsal / devlet bütçesi kısıtlamaları, risk değerlendirmeleri vb. İçinde çalışmak zorunda kalacaklardır.

# 12. Terörizm Riskini Azaltma

*Bu teröristlerin belirlenmesi Amerikan halkının tespitini caydırmayacak. Biz kurtulduk ve özgürlük kurtulan.*

*- Başsavcı John Ashcroft*

*11 Eylül 2001 tarihli basın toplantısı*

Şimdi neden daha büyük bir terörizm riskiyle karşı karşıya kaldığımızı ve kimin hedef olabileceğini daha iyi anlıyoruz, bu durum organizasyonlarımızı ve diğer çalışanlarımızı daha iyi nasıl koruyacağımıza dönüşüyor. Terörizm riskini azaltmanın birçok yöntemi var. Bu yöntemler arasında önceden tartışılan önleme paradigmasını kullanarak bir kuruluşun fiziksel güvenliğinin gözden geçirilmesi ve arttırılması; operasyonel güvenlik yoluyla hassas bilgilerin kontrol edilmesi; terör olayı ele alma prosedürlerinin geliştirilmesi; ve çalışanlar için güvenlik prosedürleri ve terörle mücadele prosedürleri oluşturmak. Bu yöntemlerin birçoğu, çalışan eğitimine ve başarılı olması için periyodik tatbikatlara dayanmaktadır.

## 12.1 Fiziksel Güvenlik Değerlendirmeleri

Riski azaltmada ilk adım, fiziksel ortamı kontrol etmektir. Bu bölümde, fiziksel güvenlik için endüstri standardı uygulamaları göstermek için standart terimini kullanıyoruz. Geliştirilmiş terimi, önleme paradigmasını içeren geliştirilmiş prosedürlere atıfta bulunacaktır.

Standart Fiziksel Güvenlik Uygulamalarının Uygulandığını Doğrulayın Standart bir fiziksel güvenlik değerlendirmesi yapın ve gereken değişiklikleri uygulayın. Fiziksel güvenlik uygulamalarının en azından mevcut standartlarda olması önemlidir. Bunu yapmak aynı zamanda çoğu kişiden gelen riski de azaltacaktır

standart fiziksel güvenlik tehditleri. Organizasyonları sorumlu tutma eğilimi bilgi güvenliğinde ortaya çıkmaya devam ettikçe, öngörülebilir gelecekte fiziksel güvenlikle de ortaya çıkması olasıdır.

Gelişmiş Bir Fiziksel Güvenlik Değerlendirmesi Yapın Standart fiziksel güvenlik uygulandığında, çok daha katı olan başka bir değerlendirme yapın. Bu değerlendirme, gelişmiş fiziksel güvenlik yöntemlerini içermelidir. Ne yazık ki, gelişmiş tehdide karşı korunmak için henüz bir dizi endüstri standardı bulunmamaktadır. ABD hükümetinden birçok mükemmel kaynak mevcuttur.

ve etkin kılar. Askeri veya diğer devlet tesislerini korumak için tasarlanmış olsalar da, bu standartların birçoğu özel sektörde de başarıyla uygulanabilir. Bu noktada, bilgi güvenliği uygulayıcıları esas olarak standartları uygulamak için kendi inisiyatiflerine bırakılmıştır. Belki yakın gelecekte, daha fazla tehdit içeren bir dizi standart geliştirilecektir.

Şu anda, İnternetten, ABD hükümetinden temin edilebilecek birçok mükemmel kaynak var. Bununla birlikte, bu yazının yazıldığı tarihte, ABD hükümeti, güvenlik nedenleriyle İnternet üzerinden kamuya hangi bilgilerin mevcut olacağı konusunda daha seçici hale geliyor. Bu kaynaklardan kaybolabilir oldukça mümkündür

İnternet yakın gelecekte bir noktada. Bilgi güvenliği uygulayıcıları kaybolmadan önce bu değerli kaynakları bulmak isteyebilirler. İnternet kaynaklarının bir listesi Ek 163.3'te bulunabilir [].

SERGİ 163.3 İnternet Kaynakları

Profesyonel organizasyonlar

DRI International - http://www.drii.org

Uluslararası Güvenlik Yönetimi Derneği - http://www.ismanet.com

Terörizm Araştırma Merkezi - http://www.terrorism.com/index.shtml

Infosyssec.com’un fiziksel güvenlik kaynağı listesi - http://www.infosyssec.com/infosyssec/physfac1.htm

Infosyssec.com’un İş Sürekliliği Planlaması Kaynak Listesi - http://www.infosyssec.net/infosyssec/buscon1.htm

Devlet kurumları

Ulusal Altyapı Koruma Merkezi (NIPC) - http://www.nipc.gov

Federal Soruşturma Bürosu (FBI) - http://www.fbi.gov

İç Güvenlik Kritik Altyapı Güvence Ofisi (CIAO) - http://www.ciao.gov

İç Güvenlik Ofisi - http://www.whitehouse.gov/homeland/

FBI’nın “Terörle Savaş” sayfası - http://www.fbi.gov/terrorinfo/terrorism.htm

Kanada Güvenlik İstihbarat Servisi (CSIS) Terörle Mücadele Sayfası - http://canada.gc.ca/wire/2001/09/110901-

US\_e.html

Alkol Bürosu, Tütün ve Ateşli Silahlar Bomba Tehdit Kontrol Listesi - http://www.atf.treas.gov/explarson/information/

bombthreat / checklist.htm

Askeri Ajanslar

Savunma Bakanlığı - http://www.defenselink.mil/

Savunma Bakanlığı’nın “Amerika’yı Savunma” sitesi - http://www.defendamerica.mil/

ABD Ordusu Fiziksel Güvenlik Alanı El Kitabı - http://www.adtdl.army.mil/cgi-bin/atdl.dll / fm/3-19.30/toc.htm

**Önerilen Değişiklikleri Uygula**

Yine, özel sektör için gelişmiş fiziksel güvenlik için tek tip standartlar olmadığı için, fiziksel güvenliğimizi arttırmak için kendi cihazlarımıza bırakıldık. Fiziksel güvenliği artırmak için sınırsız bütçeye sahip olma ihtimalimiz olmadığı için, bilgi güvenliği uygulayıcıları bu kişilerin risklerini değerlendirmek zorunda kalacaklar.

Potansiyel terör tehdidi de dahil olmak üzere örgütleri değerlendirir ve değerlendirilen riske dayanarak önerilen değişiklikler yapar. İdeal olarak, bu değişiklikler mümkün olan en hızlı şekilde uygulanmalıdır.

Operasyonel Güvenlik ile Hassas Bilgilerin Kontrolü

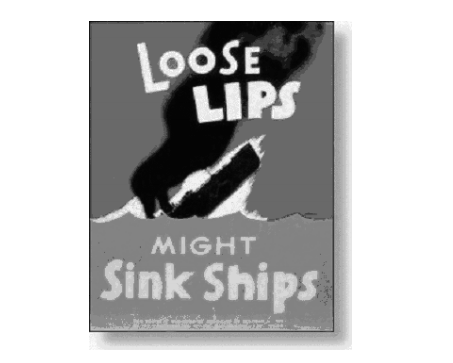
(OPSEC)

Şimdi başarıyla “vagonları daire içine aldık” ve tesislerimize fiziksel erişim kontrollerini iyileştirdik. Bir sonraki adım, hassas bilgilerimizi daha iyi kontrol etmektir. Ek 163.4'te gösterilen ünlü II. Dünya Savaşı güvenlik posterinin gösterdiği gibi, bilgilerin başarılı şekilde kontrolü savaşları kazanabilir veya kaybedebilir. Müttefik Enigma'yı ele geçirdi

şifreleme cihazı, II. Dünya Savaşı sırasında Almanlar için kritik bir darbe olduğunu kanıtladı. Müttefikler daha sonra kritik kodları çözebildi ve bu da onlara aşılmaz bir avantaj sağladı. Yine Körfez Savaşı sırasında, Müttefik Koalisyonunun sağladığı en büyük teknik avantaj, onlara hava üstünlüğüne çevrilmiş bilgi üstünlüğü verdi.

Bu tarih dersleri, hassas bilgilerin zarar vermek isteyenlerin ellerinden uzak tutulmasının önemini göstermektedir. 11 Eylül'den bu yana, bu, erişimi olmayan herkesten hassas bilgileri tutmak anlamına geliyor. İlk önce, hangi bilgilerin hassas olduğunu tam olarak tanımlamamız gerekir. O zaman hassas bilgiyi en iyi nasıl kontrol edeceğimize karar vermeliyiz.

• Hassas bilgilerin tanımlanması. Hassas bilgiler kolayca, yetkisiz bir tarafın kullanımına açıksa, güvenlik açıklarını açığa çıkarabilecek ya da diğer bilgilerle birleştirilebilecek bilgiler olarak tanımlanabilir. bir kuruma karşı kullanılmak. Örneğin, halka açık bir Web sitesinde görünüşte masum olan bilgiler, o kurumu hedeflemek için yeterli bilgi içeren düşmanca bir taraf sağlayabilir. Gibi bilgiler tesislerin adresleri, tesislerin haritaları, memur ve çalışan isimleri ile müşterilerin veya müşterilerin isimleri ve adresleri bir yol haritası oluşturmak için birleştirilebilir. Bu yol haritası potansiyelini söyleyebilir terörist sadece örgütün nerede olduğu ve ne yaptığı değil, aynı zamanda örgütün bir parçası olan ve savunmasız olduğu yerlerdir.



*SERGİ 163.4 II. Dünya Savaşı ünlü güvenlik posteri.*

• Hassas bilgilerin kontrol edilmesi. İhtiyatlı bilgi güvenliği uygulayıcıları önce kendilerini en savunmasız bırakan bilgi kaynağını kontrol etmek isteyeceklerdir. Güvenlik birkaç yöntem var uygulayıcılar hassas bilgilerinin kontrolünü sağlamak için kullanabilirler: hassas bilgilerin Web sitelerinden ve kurumsal iletişimden kaldırılması; hassas bilgilerle çöpleri imha etmek; temiz bir masa politikasına sahip olmak; ve yüklenicinin / satıcının hassas bilgilere erişimini sınırlama.

• Halka açık web sitelerinden hassas bilgileri kaldırın. Fiziksel adreslerin, haritaların, görevlilerin / çalışanların adlarının vs. bu Web sitelerinden kaldırılması şiddetle tavsiye edilir. İkisi de olabilir

Siteden tamamen kaldırıldı veya bu bilgilere erişimin doğrulandığı ve kaydedildiği sitenin güvenli bir bölümüne taşındı.

• 17 Ocak 2002 tarihinde, Ulusal Altyapı Koruma Merkezi, NIPC Danışma Belgesi 02- 001: İnternet İçerik Danışma Belgesi: İstenmeyen Kitleyi Göz önünde bulundurarak yayımladı. İçin bkz. Ek 163.5

danışma belgesinin yeniden yazdırılması. Bu danışma belgesi, halka açık İnternet sitelerinde neyin ve neyin yerleştirilmeyeceğine karar vermek için bir dizi standart olarak işlev görebilir. Bilgiyi Web sitelerinden kaldırma yönetimi ile ilgili sorunu gündeme getirirken, bilgi güvenliği uygulayıcısı danışmada yedi numaralı maddeyi tekrarlayan bir yanıt alabilir: “Bilgi, birçok yerde halka açık olduğundan, kaldırılması için çaba gösterilmeye değmez sitemizden. ”

Her ne kadar bilgi başka yerlerde bulunsa da, teröristlerin onu bulması için en muhtemel ve en kolay yer hedef kurumun Web sitesindedir. Burası aynı zamanda ilk bakacakları yer. Sorumlu bilgi güvenliği uygulayıcıları veya bu konuda şirket memurları, düşmanlık sahibi kişilerin İnternet sitelerinden yararlı bilgiler edinmelerini mümkün olduğunca zorlaştırmalıdır.

• Tüm kurumsal iletişimden hassas bilgileri kaldırın. Hiçbir kurumsal iletişim hassas bilgi içermemelidir. Bir kuruluşta zaten bir bilgi sınıflandırma yapısı varsa, bu güvenlik açığının önceden giderilmesi gerekir. Ancak, herhangi bir bilgi sınıflandırma yapısı mevcut değilse, bu böyle bir programın uygulanması için mükemmel bir gerekçedir. Ve böyle bir programla, belgeleri markalama ihtiyacı da vardır.

• Hassas bilgileri içeren çöpleri parçalayın / imha edin. Çöp kutusundan kimin geçtiğini gerçekten biliyor musun?

Janitorial ekibinizi tanıyor musunuz? Dumpster dalış, yaygın olarak uygulanan bir sosyal mühendislik yöntemidir. Parçalama, bu güvenlik açığını önlemenin mükemmel bir yoludur ve zaten yaygın şekilde uygulanmaktadır.

Birçok kuruluş, daha sonra sözleşmeli parçalama şirketleri tarafından parçalanan hassas belgeleri toplamak için yerinde parçalayıcılara veya kutulara sahiptir.

• Temiz bir masa politikası oluşturun. Masaüstünde gözetimsiz bırakılan bilgiler sosyal mühendislerin favorisidir. Çöp bidonuna dalmaktan daha kolaydır (temizleyici de!) Ve muhtemelen daha iyi sonuçlar verecektir.

Temiz masanın tanımı değişebilse de, böyle bir politikanın amacı hassas bilgilerin masaüstünde gözetimsiz bırakılmamasıdır.

• Yüklenici / satıcının hassas bilgilere erişimini sınırlandırın. Bu standart bir fiziksel güvenlik uygulamasıdır ancak OPSec kategorisinde özel olarak bahsedilmeyi hakediyor, çünkü müteahhit / satıcı erişimi üzerindeki kontrolleri uygulamak oldukça kolaydır. Özel bilgilere erişimi kısıtlamak da iyi bir uygulamadır.

Fiziksel Güvenlik: 11 Eylül 2001 1983'ten Sonra Tehdit

Ek 163.6 Güvenli Posta İşleme Kontrol Listesi

Şüpheli Paketler veya Posta

Aranacak şüpheli özellikler şunları içerir:

Alışılmadık veya bilinmeyen bir menşe yeri

Dönüş adresi yok

Aşırı miktarda posta ücreti

Olağandışı veya olağandışı boyut

Paket üzerindeki yağlı lekeler

Bir öğeye çıkıntı yapan veya ona bağlı teller veya teller

Paket etiketinde yanlış yazım

Farklı iade adresi ve posta damgası

Yabancı stil el yazısı görünümü

Kendine özgü koku (teröristler tarafından kullanılan birçok patlayıcı ayakkabı cilası veya badem gibi kokuyor)

Sıradışı ağırlık veya hafiflik

Düzensiz denge veya şekil

Üstte, altta veya yanlarda yaylanma

Asla şüpheli bir ambalajın üzerine bant, ip veya diğer ambalajları kesmeyin veya şüpheli bir mektubu veya ambalajı suya batırmayın; Her iki hareket de patlayıcı bir cihazın patlamasına neden olabilir

Şüpheli bir pakete veya mektuba asla dokunmayın veya taşımayın

Şüpheli paketleri veya postaları derhal güvenlik görevlilerine bildirin.

• Tüm bina / ofis ziyaretçilerinin kimliğini doğrulayın. Birçok büyük kuruluş ve ofis binası tüm ziyaretçilerin kimliğini doğrulamaktadır. Bazı kuruluşlar ve binalar, giren herkes için kimliği kontrol ediyor. Bu mükemmel bir uygulamadır, çünkü yetkisiz erişim riskini büyük ölçüde azaltır.

• Olağandışı ziyaretçileri veya etkinlikleri kolluk kuvvetlerine (LEA) bildir. Şüpheli veya olağandışı şekilde davranan ziyaretçilerin, mümkünse güvenliği sağladıkları ve daha sonra kolluk kuvvetlerine bildirdikleri bildirilmelidir. Hızlı raporlama, istenmeyen etkinlikleri önleyebilir.

• Güvenli posta işleme prosedürlerini uygulayın. Posta işleme prosedürleri, 2001 sonbaharında şarbon korkusu sırasında daha büyük önem kazanmıştır. Güvenli posta işleme prosedürlerinin bir listesi için bkz. Ek 163.6.

Terörizm Olayı İşleme Prosedürlerini Geliştirin

Güvenlik Çalışma Grubu

Birçok kuruluş güvenlik çalışma grupları kurmuştur. Bu gruplar yönetim, bilgi güvenliği uygulayıcıları, diğer güvenlik uzmanları ve güvenlik ve tesis yönetimi çalışanlarından oluşabilir.

Grubun üyeleri ayrıca istihbarat / tehdit bilgisi almak için yerel, eyalet ve federal otoritelerle ve profesyonel kuruluşlarla ağ oluşturmada odak noktası olarak görev yapabilir. Grup, kuruluşun güvenlik duruşunu gözden geçirmek ve yükseltilmiş güvenlik prosedürlerini uygulamak için bir organ olarak hareket etmek için düzenli olarak toplanabilir.

Ayrıca güvenlik değerlendirmeleri de yapabilir.

# 13. Terörizm Olayı Prosedürleri Oluşturma

Bilgisayar güvenlik olayları için olay müdahale planlarının ve prosedürlerinin olması önemli olduğu gibi, terör tehditleri veya olayları için olay müdahale planlarının ve prosedürlerinin bulunması da şiddetle tavsiye edilir.

Herhangi bir terör olayı tepkisinin ayrılmaz bir parçası bomba tehditleri ve diğer terörist tehditler için kontrol listeleridir.

Bu kontrol listeleri, bireye tehdit çağrısı yapmasını isteyen çok sayıda soru içermelidir: bomba nerede, ne zaman patlayacak, neye benziyor, vb. Kontrol listeleri ayrıca arayan kişinin sesinin tanımlarını doldurmak için boşluklar içermelidir. - yabancı aksan, erkek veya kadın, ses tonu, arka plan gürültüsü vb. Kontrol listeleri tüm telefonların yakınında veya en azından şirket telefon rehberlerinde bulunmalıdır.

Birçok federal ve eyalet kurumunun genel halk için bu tür kontrol listeleri vardır. Alkol Bürosu, Tütün ve Ateşli Silahlar, pek çok kurum tarafından kullanılan ve Ek 163.7'de gösterilen mükemmel bir kontrol listesine sahiptir.

Yine, bilgisayar olayı müdahale ekiplerinde olduğu gibi, eğitim oldukça önemlidir. Çalışanların bu tür yüksek stresli durumlarda nasıl cevap vereceğini bilmeleri gerekir. Tehdit altındaki telefon görüşmelerine nasıl cevap verileceği ve kontrol listesinin doldurulması konusunda tekrarlanan eğitimler risklerin azalmasına katkıda bulunuyor.

SERGİSİ 163.7 BANYO Bombası Tehdit Kontrol Listesi

ATF BOMBASI TEHLİKE KONTROL LİSTESİ

Tam görüşme süresi:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Arayanın tam kelimeleri:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

SORULAN SORULAR

1. Bomba ne zaman patlayacak?

2. Bomba nerede?

3. Neye benziyor?

4. Ne tür bir bomba?

5. Patlamasına neden olacak ne var?

6. Bombayı yerleştirdiniz mi?

7. Neden?

8. Nereden arıyorsun?

9. Adresiniz nedir?

10. İsmin nedir?

CALLER’IN SES (daire)

Sakin Yavaş Ağlama Slurred

Stutter Derin Gürültülü Kırık

Kıkırdayan Accent Angry Hızlı

Stresli Nazal Lisp Heyecanlı

Gizli Samimi Gıcırtılı Normal

Ses tanıdık geliyorsa, kime benziyordu?

Herhangi bir arka plan gürültüsü var mıydı?

Uyarılar:

Çağrı alan kişi:

Telefon numarası araması şu adresten alındı:

Tarih:

Aramayı hemen şuna bildir:

(Bomba olay planına bakınız)

Güvenlik Uygulamaları

Kurumsal güvenlik personelini veya komitelerini dahil etmek için mükemmel bir fırsat. Bazı uygulamalar

Onları dahil etmek:

• Bina tahliye prosedürlerini gözden geçirin. Bu, ihtiyaç olması halinde binaların boşaltılması için mevcut ve en iyi yöntemi sağlayacaktır. Ayrıca, birincil yolun kullanılamaması durumunda ikincil tahliye yollarını planlayın.

• Bina tahliye tatbikatları yapın. Yangın tatbikatları gibi periyodik bina tahliye tatbikatları, kaçış yolları konusunda eğitim ve tanıdıklık sağlar. Acil bir durumda, eğitime cevap vermek çok daha iyidir. Bunlar

tüm vardiyalarda önceden bildirimde bulunulmadan yapılmalıdır. Matkaplar her zaman aynı olmamalıdır.

Periyodik olarak, tahliyeleri rotalarını değiştirmeye zorlayarak bir kaçış rotasını engelleyerek tatbikatı değiştirin.

• Terörizm olayı tatbikatları yapmak. Çeşitli terör senaryolarına cevap vermek gibi diğer tatbikatlar, böyle bir durumda hızlı ve güvenli bir şekilde yanıt vermek için gerekli eğitimi sağlamada yararlı olabilir.

• Koruyucu ekipman düzenleyin. Dünya Ticaret Merkezi felaketinden kurtulanların birçoğu duman soluması, göz yaralanmaları vb. Yaşadı. Acil durumlarda bu tür yaralanmalardan kaçınılabilir.

ekipman, kask, toz maskesi, gözlük, el feneri, eldiven vb. çalışanlara verilir.

## 13.1 Bina Güvenliği Prosedürleri

Kararlı bir terörist çoğu ofis binasına nüfuz edebilir. Bununla birlikte, koruyucuların ve fiziksel güvenlik cihazlarının (örneğin dış lambalar, kilitler, aynalar, görsel cihazlar) varlığı ve kullanımı önemli bir psikolojik caydırıcıdır. Teröristler, daha az korunanlar için riskli hedeflerden kaçma eğilimindedir. Teröristler riski kabul etmeye karar verirse, güvenlik önlemleri başarı şanslarını azaltabilir. Elbette, teröristler çabalarında ölmeye istekli olursa, başarı şansları artar ve onları engelleme çabaları çok daha karmaşık ve pahalıdır. Kurumsal ve devlet yöneticileri kapsamlı bina güvenliği programları geliştirmeli ve sık sık

Etkili bir bina güvenliği programının temelini oluşturan güvenlik anketleri. Bu araştırmalar, güvenlik koşullarının ve sorunlarının, mevcut kaynakların ve potansiyel güvenlik politikasının doğru bir şekilde değerlendirilmesi için temel bilgiler üretir. Karmaşık bir yapıdaki birçok yönden yalnızca biri olan güvenlik politikaları, yangın güvenliği, normal polis prosedürleri, çalışma ortamı ve iş işlemleri gibi diğer önemli alanlarla entegre edilmelidir. Ek 163.8'de bulunan bina güvenlik kontrol listesi, bina güvenlik prosedürleri geliştirilirken rehberlik eder.

Çalışanlar İçin Terörle Mücadele Prosedürleri

Terörle Mücadele prosedürleri, terör saldırılarına karşı kırılganlığı azaltmak için kullanılan savunma önlemleri olarak tanımlanabilir.

Bu savunma önlemleri veya prosedürleri, ABD hükümeti tarafından oluşturulmuş olmasına rağmen, kesinlikle yüksek terör tehdidi koşullarında yaşayanlar için geçerlidir. Bazı güvenlik uygulayıcıları için, bu prosedürlerin çoğu paranoya eşiğinde görünebilir; bununla birlikte, iki niyetle sunulurlar: (1) var olan çeşitli tehlikeleri ve bunlardan kaçınma yöntemlerini göstermek ve (2) okuyucuların hangi prosedürlerin kullanılacağını kendileri belirleyebilmelerini sağlamak.

Prosedürlerin çoğu basitçe sağduyulu. Diğerleri ise genellikle yalnızca yüksek terör tehdidi ortamlarında yaşayan ve çalışanlar tarafından bilinen prosedürlerdir. Personel terörle mücadele kontrol listesi için bkz.

# 14. 11 Eylül'den Alınan Dersler

*Planımız işe yaradı ve yapması gerekeni yaptı. Çalışanlarımız güvenle tahliye edildi.*

*- Paul Honey*

Merrill Lynch Küresel Acil Durum Planlama Direktörü

Çok iyi hazırlanmış organizasyonlar 11 Eylül felaketini havaya kaldırdı. Ancak, hazırlıksız yakalanan birçok işletme de vardı; Bunların çoğu artık yok. ABD ve dünyanın dört bir yanından gelen organizasyonlar, o kader günü öğrenilen derslerden yararlanıyor. Bir büyük ve oldukça tanınmış

iyi hazırlanmış ve hayatta kalan organizasyon ise Merrill Lynch oldu. Merrill Lynch'in küresel acil durum planlama direktörü Paul Honey, 11 Eylül sabahı işe geldiğinde, yıkılan Dünya Ticaret Merkezinin felaketiyle karşılaştı. Bal daha sonra, acil durum planlama personelinin işinin zor olduğu şirketin acil komuta merkezlerinden birine gitti.

Felaketten bir saat sonra, kriz yönetimi ekibi kilit temsilcilerle iletişim kurmuştu ve acil durum prosedürleri yolunda gidiyordu.

Honey’in ekibi bir gün içinde kritik operasyonların sürdürülmesini ve bir hafta içinde 8000 çalışanın taşınmasını kolaylaştırdı. Bu çaba, iyi belgelenmiş ve sağlam bir iş sürekliliği programının etkinleştirilmesini, muazzam bir iletişim çabasını ve çok sayıda ekip çalışmasını gerektiriyordu.

# 15. İş Sürekliliği Planları

Bal, Merrill Lynch’in tüm işletmeleri için iş sürekliliği planlama sorumluluğuna sahiptir. İşletmenin iş sürekliliği planını veya BCP'yi takip ettiğini doğrulayan 19 kişilik bir ekibin yöneticisidir. Teknoloji kurtarma planlamasından sorumlu olmayan ekibi, ve planları yazmazlar. Program yönetiminde konu uzmanlarıdır ve tam bir BCP programı yaşam döngüsü boyunca standartları belirlerler. Planlama, programın kapsamlı olması nedeniyle şirket içinde birçok farklı departmanı içerir. Her işletme ve destek grubu (yani, ticaret katı, işlemler, finans vb.), O alandan sorumlu bir planlama yöneticisi atar.

EXHIBIT 163.8 Yapı Güvenliği Kontrol Listesi

Office erişilebilirliği

• Terörist hedef olma olasılığı en yüksek binalar halka doğrudan erişilemez olmalıdır.

• Yönetici ofisleri zemin katta bulunmamalıdır.

• Giriş kapısını, tarama personelinden ve kapıdan geçen nesnelerden sorumlu kişinin görüşüne yerleştirin.

• Elektromanyetik bir kapı kilidi takılarak kapılar uzaktan kontrol edilebilir.

• En etkili fiziksel güvenlik yapılandırması, kapıları içeriden kilitlemeli ve yürütme alanına yalnızca bir ziyaretçi erişim kapısına sahip olmalıdır. Kilitli kapıların panik çubukları da olmalıdır.

• Organizasyonun faaliyetlerinin niteliğine bağlı olarak, belirli bir ofisteki konum ve fonksiyondan dikkat çekmek için birkaç ofise erişimi kontrol eden geniş bir bekleme alanı gibi aldatma önlemleri alınabilir.

# 16. Fiziksel Güvenlik Önlemleri

• Aşağıdaki güvenlik cihazlarını kurmayı düşünün: hırsız alarm sistemleri (tercihen merkezi bir güvenlik tesisine bağlı), sonik uyarı cihazları veya diğer izinsiz giriş sistemleri, dış projektörler, kapılarda sürgü kilitleri, pencerelerde kilitler ve demir ızgaralar veya pencereler için ağır perdeler.

• Tesisin yapısına bağlı olarak, 15-20 ayak çit veya duvar ve kapsamlı bir dış aydınlatma sistemi kurmayı düşünün. Dış aydınlatma yasadışı girişe en ucuz ve en etkili engellerden biridir.

• Kurcalamayı zor ve farkedilir kılmak için aydınlatma armatürlerini yerleştirin.

• Teröristler ve diğer davetsiz misafirlere, özellikle de girişlere yakın olanlara kapalı veya gizli bir yaklaşım yolu bulunmadığından emin olmak için gerekçeleri kontrol edin.

• Yangın kaçışlarına, merdivenlere ve çatılara dıştan erişimi engelleyin.

• Binanın yakınındaki rögar kapakları emniyete alınmalı veya kilitlenmelidir.

• Dış mekan açıklıklarını örtün, kilitleyin veya ekranlayın (örneğin, kömür kutuları, havalandırma kanalları, erişim noktaları).

• Camlar (özellikle zemine yakın veya bitişik binalardan erişilebilir).

• Patlama durumunda uçan camın etkilerini azaltmak için pencerelere ince ve şeffaf bir plastik tabaka eklemeyi düşünün.

• Bodrum ve diğer nadir kullanılan alanlar dahil, tüm binanın içini düzenli olarak inceleyin.

• Bina dışı çöp konteynırlarını, depolama kutularını ve bisiklet raflarını binadan uzağa yerleştirin.

• Kitap depoları veya posta yuvaları binaya bitişik veya bina içinde olmamalıdır.

• Posta kutuları binaya yakın olmamalıdır.

• Boşlukların üst kısmını ve dolapların, kitaplıkların ve vitrinlerin üzerindeki açık alanları kapatın.

• Kapıcı dolapları, servis açıklıklarını, telefon dolaplarını ve elektrikli dolapları her zaman kilitli tutun. Haberleşme dolaplarını ve kullanım alanlarını bir alarm sistemiyle koruyun.

• Ayrılmış park yerlerinden adları kaldırın.

• Çöp haznelerini günlük olarak boşaltın (tercihen günde iki kez).

• Çalışma düzeninde ve hazır olduklarından emin olmak için tüm yangın söndürücüleri düzenli olarak kontrol edin. Çalışma düzeninde olduklarından emin olmak için tüm duman alarmlarını periyodik olarak kontrol edin.

Personel İşlemleri

• Binada çalışan personelin artan farkındalığını vurgulayın, çünkü etkili bina güvenliği büyük ölçüde insanların davranışlarına ve farkındalığına bağlıdır.

• Personel güvenliği prosedürleriyle ilgili açık talimatlar geliştirmek ve yaymak.

• Bina sakinleri için düzenli güvenlik brifingleri düzenleyin.

• Personel güvenlik önlemlerini, uygun müdahaleleri anlamalı ve acil durumlarda kiminle iletişim kuracağını bilmelidir.

• Uygunsa tatbikat yapın.

• Kıdemli personel rutin olarak geç saatlere kadar çalışmamalıdır. Hiç kimse yalnız çalışmamalı.

• Tüm personele, özellikle sekreterlere, bomba tehditleriyle ve haraç telefon görüşmeleriyle ilgili özel eğitimler verin.

Her telefonda bir bomba tehdidi kontrol listesi ve bir kalem veya kurşun kalem bulunduğundan emin olun.

• İnterkom, telefon ve zorlama alarm sistemleri bulunan üst düzey personel, sekreter ve güvenlik personeli arasında güvenli iletişim sistemlerinin varlığını sağlamak.

• Birincil iletişim sistemlerinin başarısız olması durumunda alternatif bir iletişim aracı (örneğin, iki yönlü telsiz) geliştirin.

• Gönderen veya kaynak olumlu olarak bilinmediği sürece binalarda paket veya büyük zarflar açmayın. Şüpheli bir paketin güvenlik personelini bilgilendirin.

• Posta odası personelinin bomba saptama işlemlerinde ve denetiminde eğitilmesini sağlayın.

SERGİ 163.8 Yapı Güvenliği Kontrol Listesi (devam)

• Tüm kapıları gece, hafta sonları ve bina gözetimsiz olduğunda kilitleyin.

• Anahtarların sıkı kontrolünü sağlayın. Kullanılmadığı zaman dolapları ve dolapları kilitleyin.

• Uygun olduğunda, kullanılmadığında tüm bina dinlenme odalarını kilitleyin.

• Binadaki ziyaretçilere eşlik edin ve giriş isteyen yabancıların tam kontrolünü sağlayın.

• Kabul etmeden önce kapıcıları ve ekipmanlarını kontrol edin ve işlevlerini yerine getirirken gözlemleyin.

• Resmi evrakları yetkisiz görüşlerden koruyun.

• Pozitif olarak tanımlanmadıkça ve bu bilgiye ihtiyaç duymadıkça bina personelinin yerini arayanlara açıklama.

• Telefonla bilgi verirken çok dikkatli olun.

• İsim pozisyonları ve özellikle ofis personelinin ev adreslerini veya telefon numaralarını yabancılara veya telefon arayanlara vermez.

• Teröristlerin potansiyel terör hedeflerinin adreslerini ve telefon numaralarını, kitap ve liste halinde listelemeyin.

• Seyahat planlarını veya tarifeleri ziyaretçilerin huzurunda tartışmaktan kaçının.

• Faaliyetleri gözlemlemek ve bilgi toplamak için kendilerini binaya yerleştirebilecek kamu görevlisi ekipleri olarak gizlenmiş insanlara karşı dikkatli olun.

• Park girişine veya terkedilmiş araçlara, özellikle binanın girişine yakın veya duvarların yakınında bulunan kamyonlara dikkat edin.

• Şüpheli araçların plaka numaralarını, markalarını, modellerini, yıllarını ve rengini ve yolcu tanımını not edin ve bu bilgileri amirinize, güvenlik görevlisine veya kanun uygulayıcı kurumunuza bildirin.

Giriş kontrolü

• Ziyaretçilere kapı açılmadan önce giriş kapılarına bir gözetleme deliği, interkom, görüşme ızgarası veya küçük bir açıklık takmayı düşünün.

• Ziyaretçilerle ilgilenmek için bir resepsiyon odası kullanın, böylece iç ofislere erişimini kısıtlar.

• Metal giriş cihazlarının kontrollü girişlere kurulmasını düşünün. Organizasyon dışı üyelerin binaya kutu ve paket getirmelerini yasaklayın.

• Bina alanı, kaydedilmemiş ziyaretçilerin resepsiyon görevlisinin görsel gözleminde olması ve ziyaretçilerin sıkı erişim kontrolü prosedürlerini takip etmesini sağlamak için düzenleyin.

• Binanın erişim kontrol sisteminde istisnalar yapmayın.

• İnterkomlar, erişim kontrol rozetleri veya kartlar ve kapalı devre televizyon kullanımıyla daha iyi güvenlik sağlamak için erişim kontrol sistemlerini yükseltin.

Kamu alanları

• Tüm saksı bitkilerini ve süs eşyalarını ortak alanlardan kaldırın.

• Çöp haznelerini sık sık boşaltın.

• Servis alanlarına kapıları kilitleyin.

• Tavan pencereleri dahil tavan veya zemindeki trapdoors'ları kilitleyin.

• Mobilya ve diğer eşyaların yapım veya yerleştirilmesinin patlayıcı cihazları veya silahları gizlememesini sağlayın.

• Mobilyaları duvarlardan veya köşelerden uzak tutun.

• Perdeleri, perdeleri veya kumaş örtülerini, gizlenmiş öğelerin kolayca görülebileceği şekilde değiştirin.

• Yüksek dolapların, rafların veya diğer donanımların üst kısımlarındaki kutu.

• Umumi dinlenme odalarında özel önlemler alın.

• Yaylı kapılara yaylı yatakları dinlenme odalarına yerleştirin, böylece kilitlenmediklerinde açık dururlar. Birinin kilitli bir ahırda bir cihazı gizlemesini önlemek için durakları bir iç mandalla donatın.

• Komodin su depolarındaki üst kısımlara sabit bir kaplama yerleştirin.

• Kirli havlular için açık örgülü sepet kullanın. Sık sık boşaltın.

• Kamuya açık alanlardaki muhafızların, tehlike dairesini sessizce uyarma ve yardım toplama (örneğin, ayakla çalıştırılan zil) gibi bir yolu olmalıdır.

# 17. Şüpheli Patlayıcı Bir Aygıtın Keşfi

• Şüpheli bir nesneye dokunmayın veya hareket ettirmeyin. Birinin nesnenin varlığını hesaba katması mümkünse, o kişiden sözlü bir açıklama ile tanımlamasını isteyin. Tahliye edilen personeli bölgeye geri getirmeyi gerektiriyorsa, bu yapılmamalıdır. Bir nesnenin varlığı açıklanamaz kalırsa aşağıdaki işlemleri yapın:

• Arama ekibi dahil binaları ve çevresindeki alanları boşaltın.

• Tahliye edilen alanlar şüpheli nesneden en az 100 metre uzakta olmalıdır.

• Bir kordon ve olay kontrol noktası veya ICP oluşturun.

Güvenlik Yönetimi

SERGİ 163.8 Yapı Güvenliği Kontrol Listesi (devam)

• ICP'ye bir nesnenin bulunduğunu bildirin.

• Sorgulanana kadar nesneyi yerleştiren kişiyi ICP'de tutun.

• Şüpheli nesneleri en az 100 metre mesafeye Cordon ve şüpheli araçları en az 200 metre mesafeye kordonlayın. Kimsenin kordonlu alana girmediğinden emin olun. Ulaşımı kontrol etmek ve varışta ICP sorumluluğunu kolluk makamlarına bırakmak için kordon üzerinde bir ICP oluşturmak. Kolluk kuvvetleri incelemelerini tamamlayana kadar kordonu koruyun ya da kordonun durduğunu belirtin. Tahliye edilen bir tesisin yeniden başlatılmasına izin verilmesi kararı tesisten sorumlu olan kişiye aittir.

Honey’in takımı, bir yıl boyunca ortalama olarak yaklaşık 70 acil duruma yanıt veriyor. Dünyanın dört bir yanındaki tesisler ve perakende şubeleri, deprem, fırtına, elektrik kesintileri, sel veya bomba tehdidi gibi çeşitli olaylarla karşılaşmaktadır.

Honey’in ekibi iş kesintisini planladığında, ekip iş gruplarına tesislerine erişimi olmayan ve doğal olarak bir kesinti için mümkün olan en kötü zamanda altı haftalık en kötü senaryoyu planlamalarını söylemektedir.

Planlama aynı zamanda, herhangi bir binadan - bilgisayarlardan, dosyalardan, evraklardan vb. Hiçbir şeye kesinlikle erişememeyi de içeriyor. “İnsanları alternatif siteler, hayati kayıtlar, personelin fiziksel olarak yer değiştirmesi vb. Hakkında düşünmeye zorluyoruz. teknolojinin başka bir sitede mevcut olduğundan emin olmak, ”diyor Honey.

Y2K Sonrası Geliştirilmiş Planlar ve Prosedürler

Merrill Lynch, Federal Reserve ve Federal Finansal Kurumlar Sınav Konseyi gibi düzenleyici kurumlar tarafından belirlenen standartlara uymak zorundadır. Honey, “Merrill Lynch gibi şirketlerin çok sağlam acil durum planları olacağına dair bir piyasa beklentisi var, bu yüzden muhtemelen ona saldırıyoruz ve

Orada olan herhangi bir yasal düzenleme şartının üstünde. ”BCP ekibi, yasal düzenlemeleri aşma konusundaki son çabaları Merrill Lynch'i 11 Eylül saldırılarından başarıyla kurtulmak için iyi bir konuma getirdi.

Acil Durum Planlarının Kapsamlı Testi Tüm planlar yılda iki kez test edilir ve yılda bir kez, büyük ölçekli şirket planları test edilir. Honey’in ekibi, merkezin tahliye planını yılın başlarında yeniledi. Yeni prosedürlerle yaklaşık 8000 pankart dağıtdılar. Bu pankartlar saldırı günü oldukça faydalı oldu. Ayrıca, şirketin insan kaynakları veritabanı, ekibin iş sürekliliği planlamasına aylık olarak indirilir.

yazılım programı. Bu, BCP ekibinin her binadaki mevcut tüm çalışanların sıkça güncellenen bir listesine sahip olmasını sağlar. Tüm bu hazırlık işlemleri, 11 Eylül'de iş sürekliliği planlarının etkili bir şekilde yürütülmesine neden oldu.

Terörist Saldırılara Benzer Bir Senaryo Kullanarak Son Testler

Mayıs 2001’de, Bal’ın ekibi merkezin kilit personeli için iki günlük bir planlama senaryosu düzenledi. Bu senaryo, 11 Eylül'den farklı olmasına rağmen, New York'taki büyük bir kasırga olan yıkıcı bir etki olayı ele aldı. “Kasırga senaryosu hayat kaybı açısından 9/11 trajedileriyle karşılaştırmasa da, şirketimizi aslında taşımacılıkta zorluklar açısından firmayı daha fazla etkileyen, oldukça kapsamlı iki günlük bir senaryoya soktuk. ve bölgedeki gerçek hasar, ”diyor Bal. “Yani biz gerçekten çok öyleydik

iyi hazırlanmış; zaten birçok lojistik, teknoloji ve İK tipi konu hakkında düşünen birçok insanımız vardı. ”

## 17.1 Tahliye

Kurumsal müdahale ekibi sabah saat 8: 55'te aktive olurken, Bal Kanal Caddesi'ne doğru yola çıktı. Tüm işletme destek gruplarından temsilcilerden oluşan ekip, bina yönetimi, fiziksel güvenlik personeli, medya ilişkileri, kilit teknoloji kaynakları ve kilit işletme birimleri gibi durumun değerlendirilmesinde etkilidir. Alandaki çok sayıda telekomünikasyon sorununa rağmen, ekip nihayet neler olduğunu anlamak için New Jersey, Jersey City'deki diğer komuta merkezi ile iletişim kurmak için 9: 30'da bir konferans araması yapabilir.

Honey, “Gördüğümde garip görünüyor, ancak binalara vuran uçakların dışında, bunun bir kaza mı yoksa terörist bir saldırı mı olduğunu bilmiyorduk” diyor. “Gerçekten de, o zamanki zorluk çalışanlarımızı hesaba katmak ve sonra ne olduğunu anlamaya çalışmaktı. Binalarımıza verilen zarar da bir endişe kaynağıydı. Binalarımız nasıldı? Hala ayakta mıydılar? Altlarındaki altyapının durumu neydi? ”

Çalışanlarla iletişime geçmek için çağrı ağaçları kullanılmış ve çalışanlar, bölgeden güvenli bir şekilde çıktıklarını bildirmek için yöneticileriyle nasıl iletişim kuracaklarını da biliyorlardı. Honey, “Bir binanın tipik bir tahliyesinde, çalışanlar binadan 100 metre uzaktadır ve isimlerinin listeden çıkarılmasını beklemektedir” diyor. “Burada karşılaştığımız konu, aşağı Manhattan'ın tamamının boşaltılması. Böylece çalışanlar eve gidiyor ya da başka ofislere gitmeye çalışıyorlardı - bu bizim için zor bir işti. ”Honey, anahtar çalışanların taşıdığı cüzdan kartlarının son derece yararlı olduğunu söylüyor.

“Herkes kimi ve ne zaman arayacağını biliyordu” diyor. “Bu olması gereken çok değerli bir planlama yardımcısıydı.”

Ekip çağrı ağaçları ve diğer iletişim süreçlerini başlattıktan sonra, önceden tanımlanmış süreklilik planlarını uygulamaya ve ne zaman ve hangi kritik konulara odaklanmak istediklerini değerlendirmeye başladı.

SERGİ 163.9 Personel terörle mücadele kontrol listesi

# 18. Genel Güvenlik Prosedürleri

• Ailenize ve ortaklarınıza, yabancılara kendiniz veya aileniz hakkında bilgi vermemesini sağlayın.

• Bilgi toplayıcılara gereksiz kişisel bilgiler vermekten kaçının.

• Yaşadığınız ya da işyerinize yakın tüm şüpheli kişileri rapor edin; Polise veya güvenliğe şahsın ve / veya aracın tam bir tanımını yapmayı denemek.

• Alışılmış kalıpları önlemek için günlük rutinde değişiklik yapın.

• Mümkünse, seyahat zamanlarını ve işe gidiş geliş rotalarını dalgalandırın.

• İş yeriniz dışındaki yabancılarla buluşmayı reddetmek.

• Ofisten veya evden ve tahmini varış saatinizden ayrılırken, gideceğiniz yerdeki ortaklara veya aile üyelerine her zaman tavsiyede bulunun.

• Yabancılara kapı açmayın.

• Anahtar telefon numaralarını ezberleyin - ofis, ev, polis, vb. Aile seyahat planları veya güvenlik önlemleri ve prosedürleri hakkında bilgi verirken dikkatli olun.

• Yurtdışına seyahat ediyorsanız, “Bir polise, doktora ihtiyacım var” gibi ana dilde birkaç önemli kelime öbeği öğrenin ve uygulayın.

İş seyahati

• Havaalanı İşlemleri

- Erken varmak; şüpheli etkinlik için dikkat edin.

- Uzaktan başkalarıyla göz temasını koruyan gergin yolculara dikkat edin. İnsanların neler taşıdığını gözlemleyin. Davranış, bölgedeki diğer davranışlarla tutarlı değil.

- Terminalde nerede olursanız olun, saldırı durumunda kapak için uygun nesneleri belirleyin; sütunlar, çöp kutuları, valizler, büyük ekiciler, tezgahlar ve mobilyalar koruma sağlayabilir.

- Açık alanların yakınında oyalanmayın. Bekleme odalarına, ticari mağazalara ve restoranlara hızlıca geçiş yapın.

- Güvenlik kontrol noktalarında mümkün olan en kısa sürede ilerleyin.

- Saldırganların gizlenmesini sağlayan tenha alanlardan kaçının.

- Terminalin herhangi bir yerinde gözetimsiz bagajın farkında olun.

- Şahsi eşya taşıma konusunda son derece dikkatli olun. Dizüstü bilgisayarlar için tasarlanan evrak çantaları hırsızlığı dünyadaki havaalanlarında artmaktadır; Aynı şekilde, düzgün bir şekilde korunmayan bagaj, bir teröristin taşıma çantanıza istenmeyen bir nesne veya cihaz yerleştirmesi için bir fırsat sağlar. Mümkün olduğunca, hiçbir şeyi paketlemeyin

kaybetmeyi göze alamaz; belgeler önemliyse, bir kopya çıkartın ve kopyayı taşıyın.

- Bagaj alanı bölgesini belli bir mesafeden izleyin. Kalabalık temizlenene kadar çantalarınızı geri almayın. Kalabalığın kenarındaki gümrük yollarına ilerleyin.

- Şüpheli faaliyeti havaalanı güvenlik personeline bildirin.

• Yerleşik İşlemler

- Pencere koltuklarını seçin; daha fazla koruma sağlarlar çünkü koridor koltukları korsanların koridordaki yukarı ve aşağı hareketlerine daha yakındır.

- Arka koltuklar da daha fazla koruma sağlar, çünkü genellikle kokpitin yakınında olan düşmanca eylem merkezinden daha uzaktadırlar.

- Acil çıkıştaki koltuklar kaçma fırsatı sağlayabilir.

• Otel İşlemleri

- Oda anahtarınızı her zaman kişinizin üzerinde tutun.

- Bölgede dolaşan şüpheli kişilere dikkat edin.

- Oda numaranızı yabancılara vermeyin.

- Odanızı ve kişisel efektlerinizi düzenli ve düzenli tutun; böylece kurcalanmayacak veya yerinde olmayan nesneleri göreceksiniz.

- Acil durum çıkışlarının ve yangın söndürücülerin yerlerini bilin.

- Yabancıları odanıza kabul etmeyin.

- Otel güvenlik görevlilerinin yerini belirlemeyi biliyor.

Düşük Profilde Tutun

• Kıyafetiniz, davranışlarınız ve tavırlarınız dikkat çekmemelidir.

• Yerel çevreye uyum sağlamak için çaba gösterin.

SERGİ 163.9 Personel Terörle Mücadele Kontrol Listesi (devam)

• Tanıtımdan kaçının ve büyük gruplarda dışarı çıkmayın.

• Sivil rahatsızlıklardan ve gösterilerden uzak durun.

Evde Aile İçin İpuçları

• Evin anahtarını bulundurma kısıtlayın.

• Anahtarlar kaybolursa veya çalınırsa ve önceden işgal edilmiş bir eve taşınırken kilitleri değiştirin.

• Garaj dahil bütün girişleri geceleri kilitleyin.

• Evde olsanız bile evi kilitli tutun.

• Komşularınızla dostça ilişkiler geliştirin.

• Kendine dikkat etme; komşularının saygılı olması.

• Balkonlarda ve camların yakınında sıkça maruz kalmaktan kaçının.

Şüphelenmek

• İkamet alanlarına erişim isteyen kamu görevlilerine dikkat edin; Girişe izin vermeden önce kimliklerini bir gözetleme deliğinden kontrol et.

• Seyyar satıcılara ve yabancılara karşı dikkatli olun.

• Şüpheli araçların lisans numaralarını yazın; işgalcilerin açıklamalarını not edin.

• Diğer aile üyelerinin yeri veya faaliyetleri hakkında sorularınız varsa şüpheli davranın.

• Tüm şüpheli etkinlikleri polise ya da yerel yasa uygulayıcılara bildirin.

Uzakta Olduğunuzda Güvenlik Önlemleri

• Evi canlı bir görünümle terk edin.

• Teslimatları durdurun veya bir komşunun evine posta gönderin.

• Kapılara notlar bırakmayın.

• Anahtarları evin dışına saklamayın.

• Farklı zamanlarda ve yerlerde ışıkları açmak ve kapatmak için bir zamanlayıcı (yerel elektriğe uygun) kullanın.

• Radyoyu açık bırakın (en iyi zamanlayıcı ile).

• Değerli eşyalarınızı saklayın.

• Polise veya yokluğunuzun güvenilir bir komşusuna bildirin.

Konut Güvenliği

• Dış zeminler:

- İsminizi ikamet veya posta kutunuzun dışına koymayın.

- İyi aydınlatın.

- El ile bitki örtüsü kontrolü saklanma yerlerini küçültmek.

• Giriş ve çıkışlar:

- Sürgü kilitleri olan sağlam kapılar

- Kapıdaki tek yönlü gözetleme deliği

- Işıklıklardaki çubuklar ve kilitler

- Cam kapılarda ve zemin kat pencerelerinde metal ızgara değil

dışarıdan ulaşılabilir

• Iç özellikler:

- Alarm ve dahili telefon sistemleri

- İtfaiyeciler

- Tıbbi ve ilk yardım teçhizatı

• Diğer istenen özellikler:

- Yaklaşımların net bir görünümü

- Birden fazla erişim yolu

- Sokak dışı park

- Yüksek (altı ila sekiz fit) çevre duvarı veya çit

SERGİ 163.9 Personel Terörle Mücadele Kontrol Listesi (devam)

Otopark

• Her zaman arabanızı kilitleyin.

• Mümkünse gece boyunca sokakta bırakmayın.

• Şüpheli kişileri kontrol etmeden asla çıkmayın. Şüpheniz varsa, uzaklaşın.

• Sadece kontak anahtarını park görevlisi ile birlikte bırakın.

• İzlemek için orada olmadığınız sürece, bagaja girmenize izin vermeyin.

• Garaj kapılarını asla açık veya açık bırakmayın.

• Varsa, uzak bir garaj kapısı açacağı kullanın. Arabanıza kapalı garajın güvenliğine girin ve çıkın.

Yolda

• Aracınıza girmek için binaları terk etmeden önce, şüpheli bir şey olup olmadığını belirlemek için çevreyi kontrol edin.

doğa var. Aracınızdan çıkmadan önce aynı güvenlik durumunu gösterin.

• Bir araca binmeden önce altını kontrol edin. Kablolar, bantlar veya olağandışı herhangi bir şey arayın.

• Mümkünse, işe ve eve giden rotaları değiştirin.

• Gece yolculuklarından kaçının.

• Arkadaşlarınızla seyahat edin.

• Mümkünse izole edilmiş yollardan veya karanlık sokaklardan kaçının.

• Emniyet kemerleri takılı, kapılar kilitli ve camlar kapalıyken alışılmış şekilde sürüş yapın.

• Aracınızın kutu içinde olmasına izin vermeyin; araçla aranızda en az sekiz fit aralık bırakın.

önünde; iç şeritlerden kaçının. Araba sürerken veya sürüş yaparken dikkatli olun.

İzleniyorsanız Nasıl Tepki Vereceğinizi Bilin

• Sürveyansın onaylanması için bloğu daire içine alın.

• Yüzleşmeye yol açabilecek diğer eylemleri durdurmayın veya gerçekleştirmeyin.

• Eve sürmeyin.

• Araba ve yolcuların tarifini alın.

• En yakın güvenli bölgeye git.

• Olayı polise bildirin.

Bir Saldırının Başlamasını İşaret Edebilecek Olayları Tanıma:

• Bisikletçi aracınızın önüne düşüyor.

• Bayrakçı veya arabanı durduran işçi.

• Sahte polis veya devlet kontrol noktası.

• Yolda engelli araç / kaza mağdurları.

• Sıradışı sapmalar.

• Aracınızın çarptığı bir kaza.

• Sizi içine alan arabalar veya yaya trafiği.

• Ani aktivite veya silah sesi.

Bir Araçta Saldırı Altında Ne Yapılacağını Bilin:

• Kendinizi, yolcuları veya yayaları zarar vermeden maruz bırakmadan, korna çalarak aracınıza dikkat çekmeye çalışın.

• Siz ve izleyiciniz arasına başka bir araç yerleştirin.

• Hemen dönüş ve kaçış yapmak; kaldırımı 30–45 derece açıyla, maksimum 35 mil / saat atla

• Gerekirse ram engelleme aracı

• En yakın güvenli bölgeye git

• Olayı polise bildirin

Ticari Otobüsler, Trenler ve Taksiler

• Değişken ticari ulaşım şekli.

• Meşgul durakları seçin.

SERGİ 163.9 Personel Terörle Mücadele Kontrol Listesi (devam)

• Daima aynı taksi şirketini kullanmayın.

• Tanımadığınız birisinin sizi belirli bir kabine yönlendirmesine izin vermeyin.

• Taksinin lisanslı ve emniyetli bir donanıma sahip olduğundan emin olun (en azından emniyet kemerleri).

• Ehliyet üzerindeki sürücü ve resmin aynı olduğundan emin olun.

• Bir arkadaşınızla seyahat etmeye çalışın.

• Mümkünse, taksinin izlemesini istediğiniz rotayı belirtin.

Giyim

• Yurtdışında ticari taşıma kullanırken veya bir bağlantı kurmak iseniz koruyucu giysilerle seyahat edin.

yüksek riskli bir alanda ticari bir terminalde uçuş.

• ABD tarafından tanımlanmış kovboy şapkaları veya botları, beyzbol şapkaları, Amerikan logo tişörtleri, ceketler veya

sweatshirt.

• Görünür bir ABD bağlantılı dövmeniz varsa, uzun kollu bir tişört giyin.

Saldırı Yapılan İşlemler

• Kapak için dalın. Koşma. Koşmak şarapnel parçasının hayati organlara ya da kafaya vurma olasılığını arttırır.

• Hareket etmeniz gerekirse, göbek taraması veya yuvarlanma. Kullanılabilir kapağı kullanarak zemine alçakta kalın.

• El bombası görürseniz, zemin üzerine düz bir şekilde, ayakları ve dizleri el bombası ile birlikte tabanlarla birlikte sıkıca yerleştirin. Bunda

pozisyonunuz, ayakkabılarınız, ayaklarınız ve bacaklarınız vücudunuzun geri kalanını korur. Şarapnel, koni içinde

patlama, vücudunu geçiyor.

• Akciğerlerinizi, kalbinizi ve göğsünüzü korumak için göğüs kafenizin yanına kollar ve dirsekler yerleştirin. Kulaklarını kapat ve

ellerinizi boynu, atardamarları, kulakları ve kafatasını korumak için kullanın.

• Yanıt veren güvenlik personeli sizi saldırganlardan ayırt edemez. Onlara yardım etmeye çalışmayın

herhangi bir şekilde. Ayağa kalkması söylenene kadar dur.

Kaçırıldıysa İşlemler

• Sakin olun, kibar olun ve esirlerinizle işbirliği yapın.

• Tüm hava korsanlarının aynı anda kendilerini açığa vurmayacaklarının farkında olun. Yalnız bir hava korsanı çıkarmak için kullanılabilir.

diğer hava korsanları tarafından nötralizasyon için güvenlik personeli.

• Genel bir kimlik belirleme talebine cevaben turist pasaportunuzu teslim edin.

• Hiçbir bilgi sunma.

• Ani vücut hareketleri, sözlü açıklamalar veya düşmanca bakışlarla kendinize dikkat çekmeyin.

• Kendinizi olası sözlü ve fiziksel istismar, yiyecek ve içecek eksikliği ve sağlıksız koşullar için hazırlayın.

• İzin veriliyorsa, zamanınızı korumak için okuyunuz, uyuyun veya yazın.

• Elçilerinizi dikkatlice gözlemleyin ve fiziksel açıklamalarını ezberleyin. Ses kalıplarını ve dili dahil et

giyim ve eşsiz fiziksel özelliklerin yanı sıra farklılıklar.

• Herhangi bir kurtarma girişimi ile işbirliği yapın. Yükselmesini söyleyene kadar yere yat.

# 19. Kurtarma

Dakikalar İçinde Devam Eden Kritik Yönetim Fonksiyonları

Şirketin kurtarma prosedürlerinin çoğu, bölgenin dışındaki Merrill Lynch tesislerindeki yedek veri merkezlerine dayanıyordu. Veri kurtarma prosedürleri olaysız takip edildi. Şirketin sıcak bir site sağlayıcısı var, ancak bu hizmeti kullanmak zorunda olmadılar.

Şirketin Y2K için hazırlık çalışmaları, kritik verilerin rutin olarak kurtarılmasına neden oldu. Honey, “Çok büyük bir BT felaket kurtarma programına sahiptik” diyor Bal ve “Birkaç yıldan beri, işletme prosedürlerini gerçekten kullanmaya yönelik prosedürleri güçlendirmek için çalışıyoruz. Bu yüzden, yedekleme veri merkezleri, fiber kanallar üzerinden yansıtma, vb. - hepsi oldukça iyi sonuç verdi. ”Aynı şekilde, komuta merkezlerindeki kurtarma personeli için:“ Bir çok insan zaten bir komuta merkezinin ne olduğunu, neden orada olmak zorunda olduklarını biliyordu. ve onlar ne

yapmamız gerekiyor, çünkü Y2K sırasında bunu yaşadık ve yaptığımız için minnettarım. ”

8000 Çalışan Bir Hafta İçinde İşe Geri Dönüyor BCP ekibinin en büyük zorluklarından biri, yerinden olmuş kişilerin işe geri dönmesi oldu. İlk olarak, şirket New Jersey'de iki kampüs tesisini kullanabildi. Şirket ayrıca emlak departmanını kalem haline getirdi.

üç durumlu alanda bulunan her boş alan ve onu bir listeye koyun. Honey’in ekibi gereksinimleri topladı ve her bir iş birimine uygun alan tahsisini koordine etti. Şirket oldukça kapsamlı bir alternatif iş düzenleme programı yürütüyor, bu nedenle bazı çalışanların evden çalışmalarına izin verildi. En sonunda,

Ekip, yurtdışındaki bazı işleri veya iş yükünün bir kısmını etkilenen çalışanlardan alan diğer Merrill Lynch ofislerine transfer edebildi.

## 19.1 Normal İşlemlere Devam Etme

Haftanın sonunda, BCP ekibinin önceliği, tüm çalışanlarla iletişim kurabildiklerinden emin olmak için değişti. İşçilerin şirketin krizi ele aldığından ve yerinden edilmiş işçilere alan tahsis edildiğinden emin olmaları gerekiyordu. Daha fazla bilgi için nereye başvuracaklarını ve hangi insan kaynakları hattını arayabileceklerini bildiren mesajlar gönderildi.

Merrill Lynch’in başkanı, CEO’su ve üst düzey iş ve teknoloji yöneticileri önceden kaydedilmiş mesajlar yaptı

Özel bir acil durum iletişim sistemi kullanılarak olaydan etkilenen tüm çalışanlara otomatik olarak gönderildi. Bu, felaketten sonraki ilk hafta boyunca yaklaşık 74.000 telefon görüşmesine neden oldu. Bal, “Bu çok önemli bir parçasıydı” diyor. “Çalışan tabanımıza doğru bilgi edinmek, basında çok fazla yanlış bilgi olması nedeniyle işi zorlaştırdı. Ayrıca, önemli iş milleti, tüm önemli müşterilerimizi aramak ve Merrill Lynch'in işletmeye açıldığına dair doğru bilgilerle güvence vermek için büyük çaba sarf etti. ”

Kilit bir lojistik zorluk, yerinden edilmiş binlerce işçiyi yeni çalışma yerlerine götürmesiydi. Şirket, şehirdeki çeşitli noktalardan diğer noktalara bir dizi feribot ve otobüs işletti. Şirket İnternet sitesi, taşıma bilgilerini etkilenen çalışanlara iletmek için de kullanılmıştır.

# 20. Dersler öğrenildi

Bal ve ekibi, önümüzdeki aylarda planlarının belirli yönlerini, bu kadar yıkıcı bir olaydan kurtarma başarısındaki başarılarından sonra bile, “Gelecekte çok daha fazla konsantre olacağımızı düşündüğüm şeylerden biri bölge- geniş felaketler. Örneğin, çok fazla değil, 'Binanız yıkıldı ve içeri giremezsiniz', ama belki 'İçinde bulunduğunuz şehir önemli şekillerde etkilenir.' Yani, nasıl olduğumuzu görmeye çalışacağız. bir binanın değil, bir binanın etkilendiği yerler açısından firmayı daha sağlam kılabilir ”dedi.

Bal ayrıca birçok şirketin gayrimenkul stratejilerini yeniden değerlendireceğine inanıyor. “Bütün operasyonlarını gerçekten tek bir binada yapmak istiyor musun?” Diye soruyor. “Neyse ki, Merrill Lynch gibi bir şirket için kullanabileceğimiz çok sayıda gayrimenkul seçeneğimiz var.”

## 20.1 Önümüzdeki Çalışma

BCP ekibi, ikinci haftanın sonuna kadar yedekleme tesisleri için yedekleme planları üzerinde çalışmakla meşguldü, birincil bölgeler de temizlendi veya satın alındı. “Operasyonlarımızın çoğu yedekleme modunda” diyor Bal, “Yedekleme planları için yedekleme planları denemek ve geliştirmek için çok çalıştık. Bu büyük bir zorluktu. ”

Şimdi takım, kendi zorluklarını ortaya koyan birincil sitelerin yeniden başlatılması için planlama aşamasındadır. Birincil tesislere geri dönülmesi yalnızca çalışanların hasarlı tesisleri yeniden yerine getirmesi tamamen güvenli olduğunda yapılmalıdır.

Bal ve ekibi için en önemli şeylerden biri, saldırıyı takip eden Pazartesi sabahına kadar her şeyin normal operasyonların yaklaşık yüzde 95'ine döndüğü idi. Geçtiğimiz birkaç yıl boyunca bu büyüklükteki bir kesintiye hazırlık çabaları karşılığını verdi. Bal, “Kesinlikle benim bakış açımdan, şirketi Mayıs ayında yapılan eğitim alıştırmasıyla yaptığımız için çok mutlu oldum” diyor. “Yapmaları gerekenler konusunda çok sayıda kilit yöneticiyi aydınlattı, bu yüzden çok hazırlıklıydık. Çoğu insan biliyordu

ne yapacağım, bu bana çok güven vericiydi. ”

# 21. Sonuç

Fiziksel güvenlik tehditlerine karşı kırılganlığın azaltılması 11 Eylül 2001'den sonra çok daha karmaşık hale geldi.

Terörizmin şimdi tüm fiziksel güvenlik planlamasına dahil edilmesi gerekiyor. 11 Eylül olayları, düşman niyetinde olanları caydırmak için tasarlanan prosedürlerin intihar teröristlerine karşı etkisiz olabileceğini gösterdi.

Fiziksel güvenliğin şu anda işletme paradigmasını caydırıcılıktan değiştirerek terörizm riskini azaltma önlemine dönüştürmesi gerekiyor. Düşmanlık eylemlerini önlemek için onları caydırmak yerine ek önlemler almak çok daha zor ve maliyetlidir, ancak zorunludur. Örgütlenme, çalışma arkadaşları ve ailesini terörizmden korumak eğitim ile mümkündür. Teröristler tarafından kullanılabilecek hassas bilgilere erişimin kontrolünü sağlamak çok önemlidir. Birçok hükümet İnternet sitesi terörizmle mücadelede faydalı olabilecek bilgilerle doludur. Ne yazık ki, bu Web sitelerinin birçoğu bu bilgileri güvenlik açıklarını bulmak için bu bilgileri kullanabilecek potansiyel teröristlere de sağlayabilir.

**İthaf**

Bu bölüm, 11 Eylül 2001 olaylarından hayatları kaybedilen veya etkilenenlere saygılı bir şekilde ithaf edilmiştir. Yazarın, bu bölümde sunulan bilgilerin bu tür başka bir olayın olasılığını azaltmada yardımcı olacağına dair en büyük umudu vardır.

# 22. Kaynakça

[1] NIPC Danışmanlığı 02-001: İnternet İçeriği Danışmanlığı: İstenmeyen Kitleyi Göz önünde bulundurarak, Ulusal Altyapı Koruma Merkezi, 17 Ocak 2002.

[2]Hizmet Üyesinin Kişisel Koruma Kılavuzu: Terörle Mücadele için Bir Kendi Kendine Yardım El Kitabı, ABD Genelkurmay Başkanları, Birleşik Personel Rehberi 5260, Temmuz 1996.

[3] Birleşik Terörizmle Mücadele için Taktikler, Teknikler ve Prosedürler, ABD Genelkurmay Başkanları, Joint Pub 3-07.2, 17 Mart 1998, Ek.

[4] ATF Bombası Tehdit Kontrol Listesi, ATF-F 1613.1, Alkol Bürosu, Tütün ve Ateşli Silahlar, Haziran 1997.

[5] Merrill Lynch, Saldırı Tutanakları İçindeki Kritik İşletme İşlevlerine Devam Ediyor, Janette Ballman, Afet Kurtarma Dergisi, 14, 4, s. 26, Güz 2001.

[6] Authentication and key distribution in computer networks and distributed systems Rolf Oppliger

[7] Anonymous Two-Factor Authentication in Distributed Systems: Certain Goals Are Beyond Attainment