Güvenlik Yönetimi, Uygulama Geliştirme Güvenliği, İş Sürekliliği Planlaması

Dr. Gülbahar
AKGÜN

İş Sürekliliği Planlaması

İş sürekliliği planlaması (Business Continuity Planning - BCP), işletmelerin operasyonlarını kesintiye uğratacak olaylara karşı hazırlıklı olmalarını ve iş süreçlerini hızla yeniden devreye alabilmelerini sağlayan stratejik bir yaklaşımdır.

İş sürekliliği planlaması, beklenmeyen durumların iş üzerindeki etkilerini azaltmak, çalışanları ve varlıkları korumak ve itibar kaybını önlemek için kritik önem taşır. İş sürekliliği planlaması aşağıdaki temel başlıklar çerçevesinde incelenebilir:

Risk Değerlendirmesi

ve

İş Etki Analizi

(Business Impact Analysis - BIA)

1. Risk Değerlendirmesi

Risk değerlendirmesi, işletmenin karşı karşıya kalabileceği tehditlerin belirlenmesi ve bu tehditlerin iş operasyonlarına olası etkilerinin analiz edilmesi sürecidir. Amaç, bu tehditlere karşı uygun önlemleri alarak riskleri azaltmaktır.

Adımları:

1. Tehditlerin Tanımlanması:

- Fiziksel tehditler: Doğal afetler (deprem, sel, yangın), hırsızlık, sabotaj.
- Teknik tehditler: Sistem arızaları, siber saldırılar, veri kaybı.
- İnsan kaynaklı tehditler: İnsan hataları, grevler, iş gücü eksikliği.
- Tedarik zinciri tehditleri: Tedarikçi hataları, lojistik sorunlar.

2. Zafiyetlerin Analizi:

- İşletmenin hangi alanlarının bu tehditlere karşı savunmasız olduğu belirlenir. Örneğin, yedekleme sisteminin olmaması, güvenlik protokollerinin eksikliği vb.

3. Riskin Değerlendirilmesi:

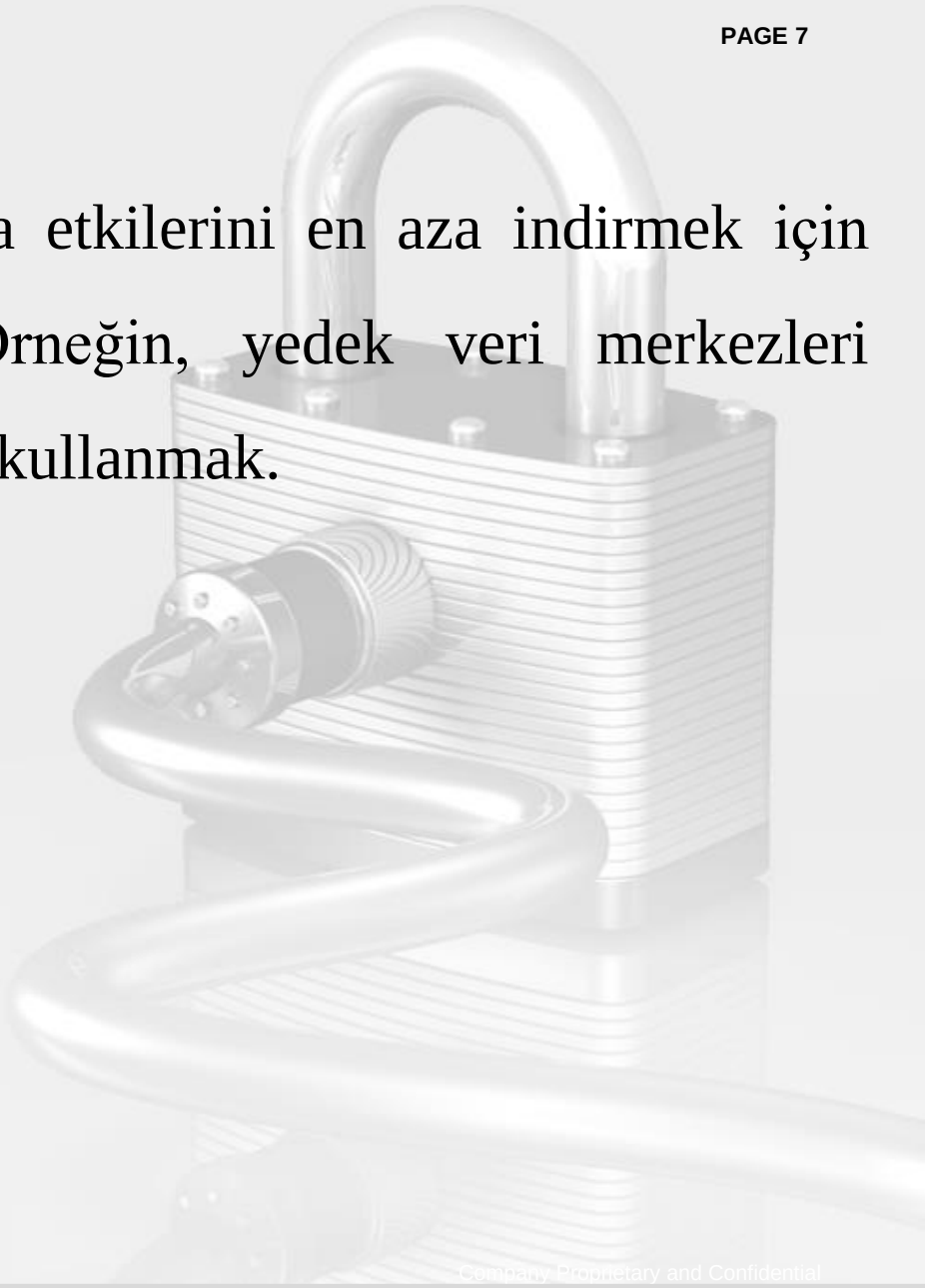
- Her bir tehdit için olasılık ve etkiler belirlenir. Bu değerlendirme genellikle bir **Risk Matrisi** kullanılarak yapılır:
  - **Olasılık (Low/Medium/High)**
  - **Etkiler (Low/Medium/High)**

4. Önceliklendirme:

- Yüksek olasılık ve yüksek etkiye sahip tehditlere odaklanılır.

5. Risk Azaltma Stratejileri:

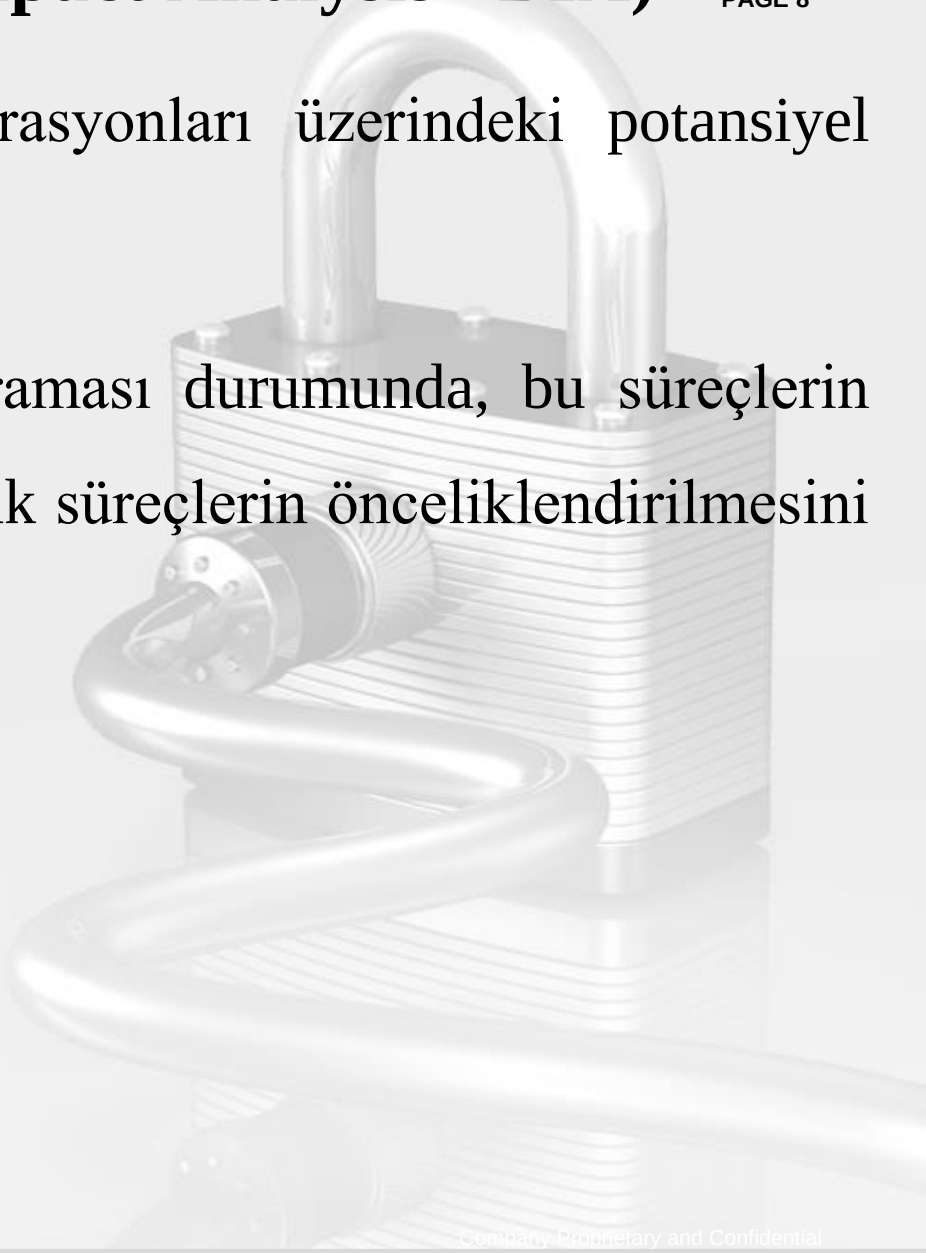
- Riskleri ortadan kaldırmak ya da etkilerini en aza indirmek için alınacak önlemler belirlenir. Örneğin, yedek veri merkezleri oluşturmak ya da güvenlik duvarı kullanmak.



2. İş Etki Analizi (Business Impact Analysis - BIA)

BIA, belirli bir kesintinin iş operasyonları üzerindeki potansiyel etkilerini analiz etme sürecidir.

Amaç, iş süreçlerinin kesintiye uğraması durumunda, bu süreçlerin işletme üzerindeki maliyetini ve kritik süreçlerin önceliklendirilmesini anlamaktır.

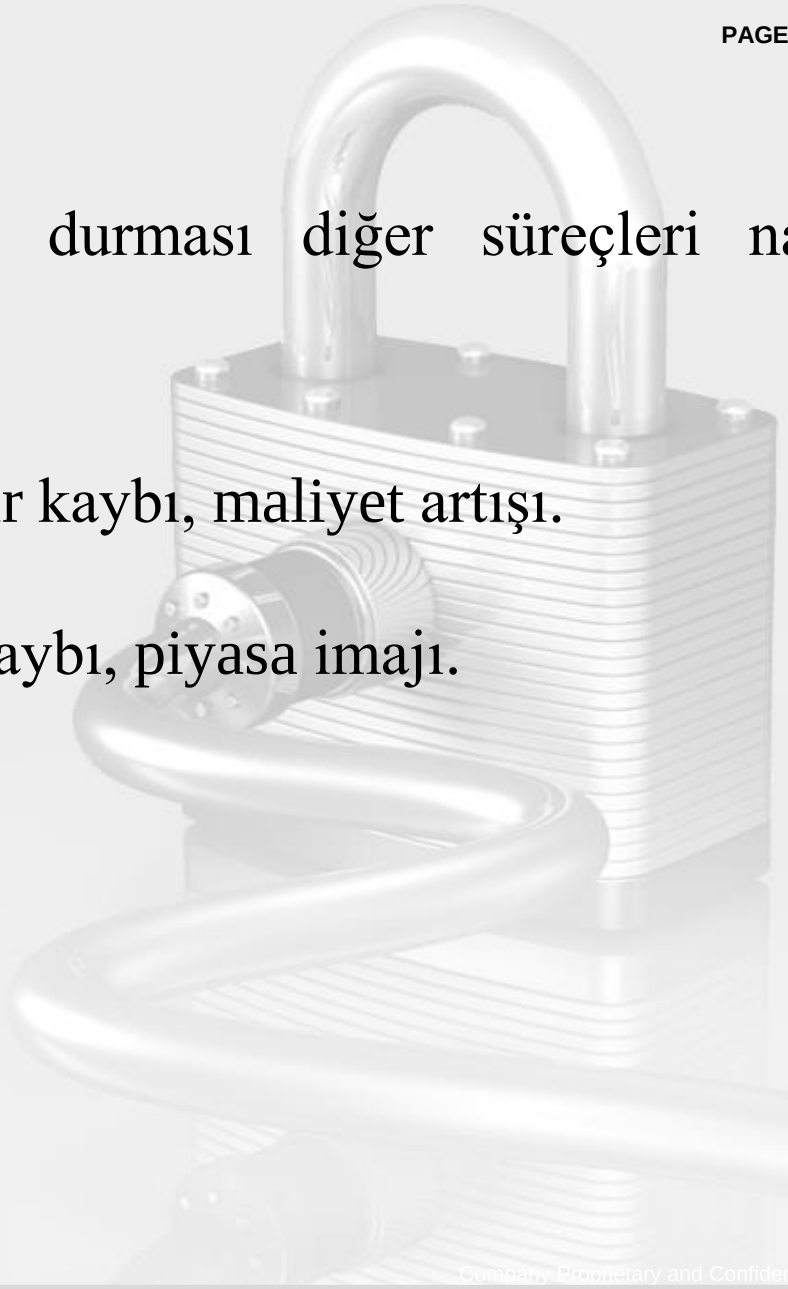


Adımları:

1. **Kritik Süreçlerin Belirlenmesi:**
   - İşletmenin hangi süreçlerinin kritik olduğunu tespit etmek. Örneğin:
     - Üretim süreçleri
     - Müşteri hizmetleri
     - Muhasebe ve faturalandırma
     - IT sistemleri.

2. Kesintinin Etkilerinin Analizi:

- Operasyonel etkiler: Sürecin durması diğer süreçleri nasıl etkiler?
- Finansal etkiler: Doğrudan gelir kaybı, maliyet artışı.
- İtibar etkileri: Müşteri güven kaybı, piyasa imajı.



3. RTO ve RPO Değerlerinin Belirlenmesi:

- **Recovery Time Objective (RTO):** İşlemlerin ne kadar süre içinde yeniden başlatılması gerektiği.
- **Recovery Point Objective (RPO):** Verilerin en son hangi noktaya kadar kurtarılabileceği.

4. Kaynak Gereksinimlerinin Analizi:

- Kesinti durumunda gerekli ekipman, personel ve diğer kaynakların belirlenmesi.

5. Önceliklendirme:

- İşletme için kritik olan süreçlerin öncelik sırasına konulması.

Risk Değerlendirmesi ve BIA'nın Faydaları:

- **Riskleri Önceden Belirler:** İşletmenin karşı karşıya olduğu tehditleri anlamayı sağlar.
- **Hazırlıklı Olmayı Sağlar:** Kritik süreçlerin korunması için planlama yapmayı mümkün kılar.
- **Kaynakların Etkin Kullanımını Sağlar:** Kritik önceliklere odaklanarak maliyet etkin çözümler geliştirir.
- **İtibar Korunur:** Müşterilere ve paydaşlara karşı güven sağlayarak işletmenin itibarını korur.

Acil Durum Planlaması

ve

Kurtarma Stratejileri

Acil durum planlaması ve kurtarma stratejileri, felaket veya beklenmedik olayların gerçekleşmesi durumunda iş süreçlerini hızlı bir şekilde yeniden başlatmak ve en az kesintiyle devam etmek için tasarlanır.

Bu planlama, kriz anında alınacak kararlar ve eylemler için yol gösterici bir rehber niteliğindedir.

1. Acil Durum Planlaması

Acil durum planlaması, işletmelerin kriz anlarında etkili bir şekilde yanıt vermek için prosedürler, kaynaklar ve roller oluşturmasını içerir. Amaç, insan hayatını ve işletme varlıklarını korumak, olayın etkilerini kontrol altına almak ve kritik operasyonların devamlılığını sağlamaktır.

Acil Durum Planlamasının Adımları:

1. Tehditlerin ve Senaryoların Tanımlanması:

- Hangi tür olaylara hazırlıklı olunması gerektiği belirlenir (doğal afetler, yangınlar, siber saldırılar, pandemiler, vb.).
- Her tehdit için olası senaryolar geliştirilir.

2. Acil Durum Ekibinin Oluşturulması:

- Acil durum yönetimi için bir ekip atanır.
- Her ekip üyesinin rolü ve sorumlulukları açıkça tanımlanır.

3. İletişim Protokollerinin Geliştirilmesi:

- Acil durum anında kimlerin bilgilendirileceği ve iletişimin nasıl sağlanacağı belirlenir.
- Telefon ağları, e-posta zincirleri ve alternatif iletişim yöntemleri tasarlanır.

4. Tahliye ve Güvenlik Planlarının Hazırlanması:

- Çalışanların ve ziyaretçilerin güvenli bir şekilde tahliye edilmesini sağlayacak planlar hazırlanır.
- Güvenli toplanma alanları belirlenir ve bu alanlara yönlendirme prosedürleri geliştirilir.

5. Acil Durum Ekipmanlarının ve Kaynaklarının Sağlanması;

- İlk yardım çantaları, yangın söndürücüler, jeneratörler, yedek su ve gıda kaynakları gibi ekipmanların yerleştirilmesi.
- Kritik iş süreçlerini destekleyecek yedek BT altyapısının sağlanması.

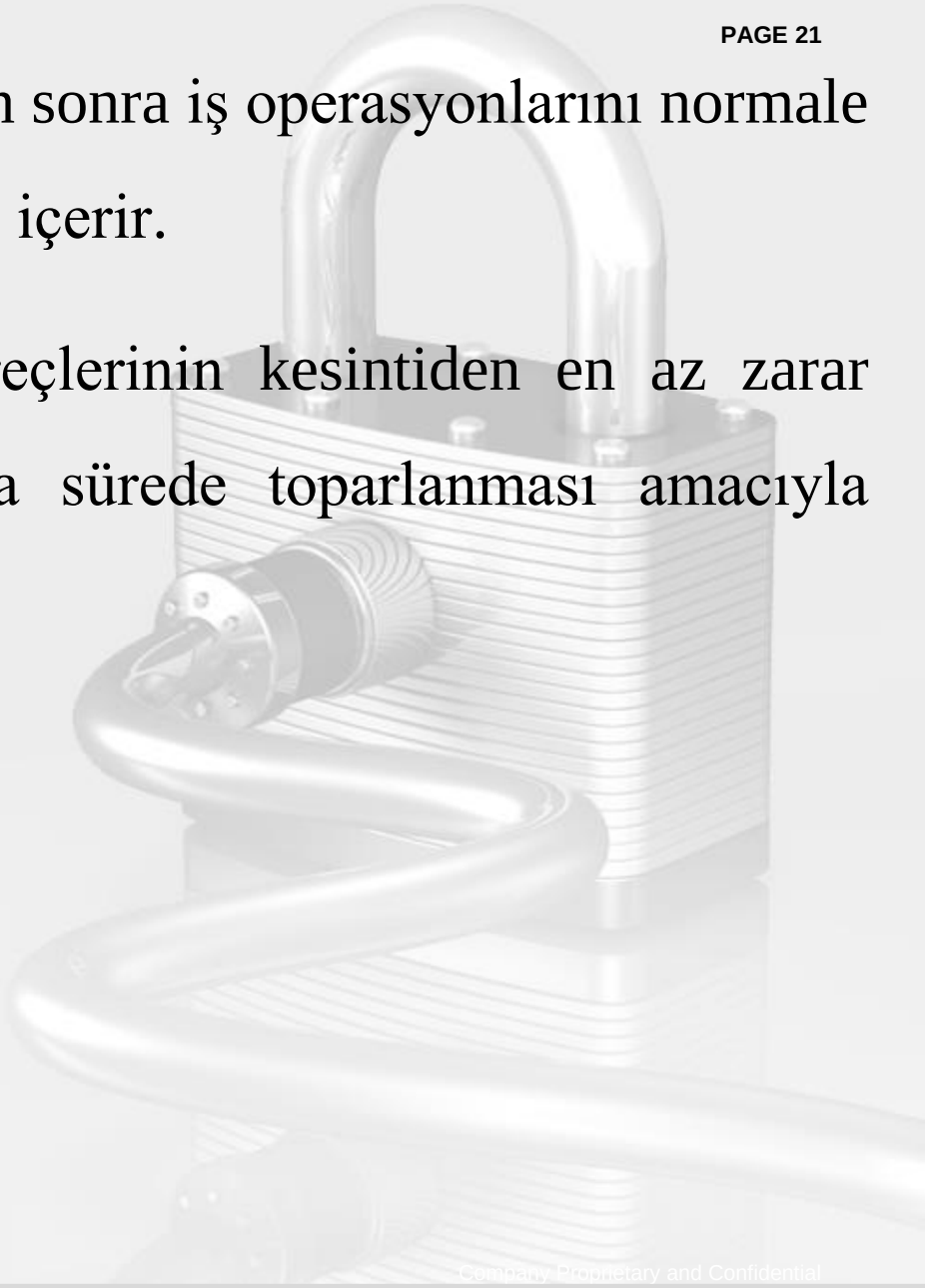
6. Eğitim ve Tatbikatlar:

- Çalışanların plana aşina olmaları ve bu planı uygulayabilmeleri için düzenli eğitimler ve tatbikatlar gerçekleştirilir.
- Olası senaryolarda planın ne kadar etkili olduğu test edilir.

Kurtarma Stratejileri

Kurtarma stratejileri, bir kesintiden sonra iş operasyonlarını normale döndürmek için izlenecek yöntemleri içerir.

Bu stratejiler, işletmenin kritik süreçlerinin kesintiden en az zarar görmesi ve mümkün olan en kısa sürede toparlanması amacıyla geliştirilir.



Kurtarma Stratejilerinin Bileşenleri:

1. Kurtarma Planları:

- İşletmenin farklı bölümleri (BT, insan kaynakları, üretim vb.) için özelleştirilmiş kurtarma planları hazırlanır.
- Planlar, her bölümün kritik süreçlerini ve bunların toparlanma yöntemlerini tanımlar.

2. Yedekleme Sistemleri ve Veri Kurtarma:

- **Veri Yedekleme:** Tüm kritik verilerin düzenli olarak yedeklenmesi.
  - Yerel yedekleme: Şirket içi sunuculara yedekleme.
  - Bulut yedekleme: Çevrim içi ve güvenli bir platforma yedekleme.
- **Kurtarma Planı:** Verilerin kurtarılması için RTO (Recovery Time Objective) ve RPO (Recovery Point Objective) hedeflerinin belirlenmesi.

3. Alternatif İş Yerleri:

- İşletme binasının kullanılamaz hale gelmesi durumunda çalışmaya devam etmek için geçici iş yerleri planlanır (örneğin, başka bir ofis veya uzaktan çalışma modeli).

4. Süreç Yedekleme ve Dış Kaynak Kullanımı:

- Kritik iş süreçlerinin yedeklenmesi veya dış kaynak kullanımı ile yürütülmesi sağlanır.

Örneğin, üretim süreçlerini başka bir tedarikçiye devretmek.

5. İkame Sistem ve Donanım Planları:

- Arızalanan makinelerin veya sistemlerin yerine kullanılabilecek alternatif ekipmanların temini.
- BT altyapısının hızla devreye alınması için yedek sunucu ve ağların sağlanması.

6. Personel Kurtarma Stratejileri:

- Acil durumda çalışanların görev dağılımlarının yeniden düzenlenmesi.
- Kritik rolleri yerine getirebilecek yedek personelin belirlenmesi.

Test ve Güncelleme

Acil durum planlarının ve kurtarma stratejilerinin işe yararlılığını garanti altına almak için düzenli olarak **test** edilmesi gerekir.

Ayrıca, işletme süreçlerindeki değişikliklere uyum sağlamak için bu planlar periyodik olarak gözden geçirilip güncellenmelidir.

Test Yöntemleri:

- **Masaüstü Tatbikatları:** Planların gözden geçirilerek senaryo bazlı analiz yapılması.
- **Tam Ölçekli Tatbikatlar:** Planların gerçek senaryoları simüle ederek test edilmesi.

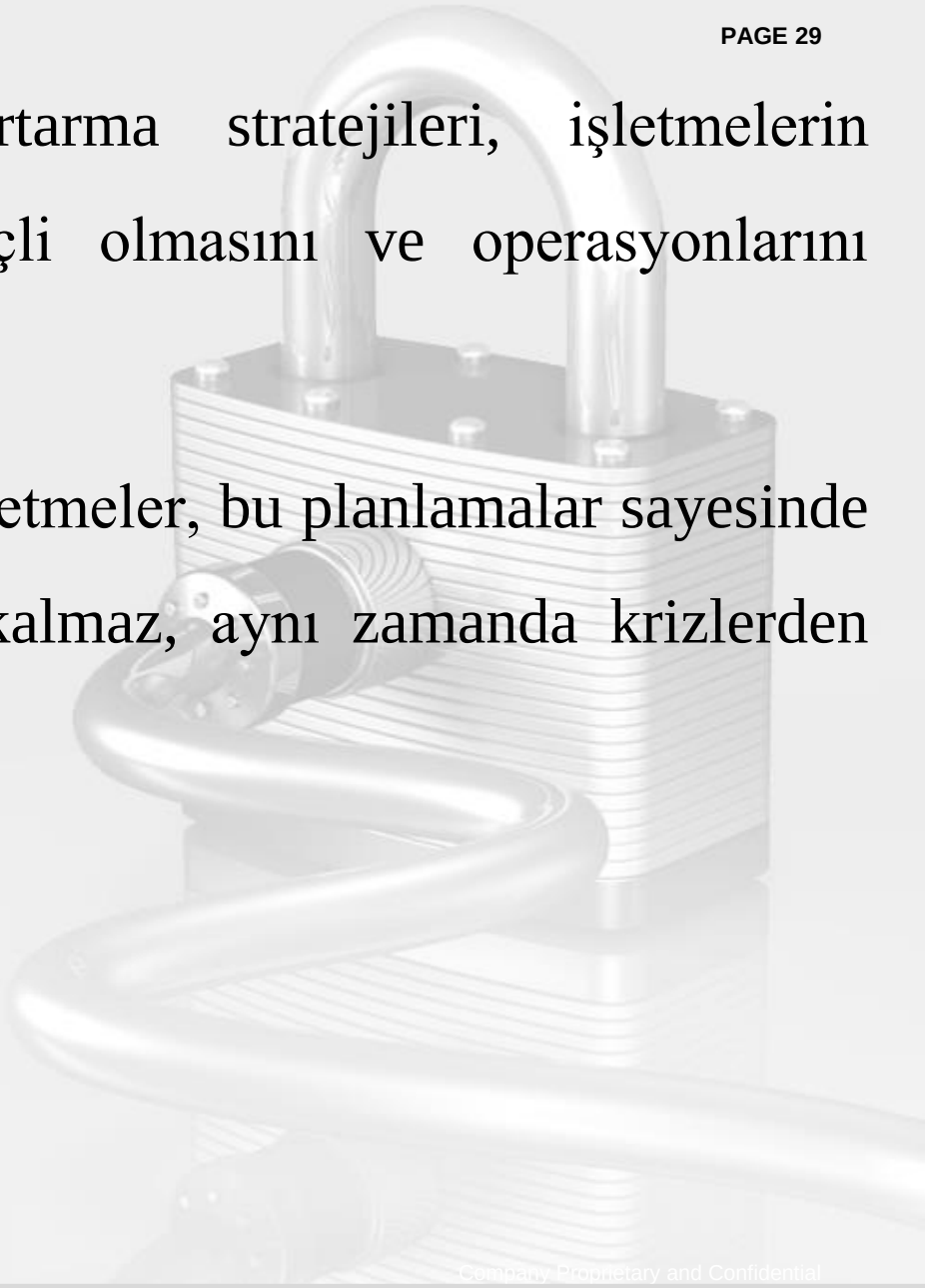
Acil Durum Planlaması ve Kurtarma Stratejilerinin Faydaları

1. **Hızlı Müdahale:** Acil durumlarda hızlı ve etkili bir şekilde hareket etmeyi sağlar.
2. **Kayıpların Azaltılması:** İnsan hayatını, varlıkları ve verileri korur.
3. **İş Sürekliliğinin Sağlanması:** Operasyonların minimum kesinti ile devamını destekler.
4. **Rekabet Avantajı:** Krizlere karşı hazırlıklı bir işletme, itibarını ve müşteri güvenini korur.
5. **Uyum ve Yasal Gereklilikler:** Düzenlemelere ve standartlara uygun bir yapı sağlar (ör. ISO 22301 - İş Sürekliliği Yönetim Sistemi).

Özetle,

Acil durum planlaması ve kurtarma stratejileri, işletmelerin beklenmeyen olaylara karşı dirençli olmasını ve operasyonlarını sürdürebilmesini sağlar.

Proaktif bir yaklaşım benimseyen işletmeler, bu planlamalar sayesinde yalnızca kriz anlarını yönetmekle kalmaz, aynı zamanda krizlerden güçlenerek çıkabilir.



Alternatif Çalışma Yerleri

ve

Yedek Sistemler

İş sürekliliği planlamasının kritik bir parçası olan **Alternatif Çalışma Yerleri** ve **Yedek Sistemler**, bir kesinti durumunda iş operasyonlarının devam etmesini sağlamak için geliştirilmiş stratejilerdir.

Bu sistemler, özellikle doğal afetler, altyapı arızaları, siber saldırılar veya fiziksel erişim kaybı gibi durumlarda işletmenin etkili bir şekilde çalışmasını sağlar.

1. Alternatif Çalışma Yerleri

Birincil iş yeri kullanılamaz hale geldiğinde, iş operasyonlarının sürdürülebilmesi için önceden planlanmış alternatif mekanlar kullanılır. Bu çalışma yerleri, işletmenin kesintiye uğramaması için kritik öneme sahiptir.

Alternatif Çalışma Yerleri Türleri:

1. Sıcak (Hot) Siteler:

Tanım: Tüm sistemlerin ve altyapının anında çalışır durumda olduğu yerlerdir.

Avantajları:

- Kesinti durumunda iş operasyonlarına neredeyse anında devam etme imkanı sağlar.
- Kritik veriler ve sistemler önceden senkronize edilmiştir.

Dezavantajları:

- Yüksek kurulum ve bakım maliyetleri.

Örnek Kullanım: Finans kurumları, sağlık kuruluşları ve büyük e-ticaret firmaları gibi anında operasyon gerektiren işletmeler.

2. Ilık (Warm) Siteler:

Tanım: Bazı temel sistemlerin ve verilerin önceden kurulu olduğu ancak tam anlamıyla çalışmaya hazır olmayan yerlerdir.

Avantajları:

- Daha düşük maliyetlidir.
- Sıcak sitelere göre hazırlık süresi biraz daha uzundur ancak hâlâ hızlı toparlanma sağlar.

Dezavantajları:

- Bazı sistemlerin ve ekipmanların eksik olması nedeniyle operasyonel gecikmeler yaşanabilir.

3. Soğuk (Cold) Siteler:

Tanım: Fiziksel bir yerin ayrıldığı ancak sistemlerin ve altyapının önceden kurulmadığı çalışma yerleridir.

Avantajları:

- Düşük kurulum ve bakım maliyeti.

Dezavantajları:

- Kesinti durumunda tam operasyon için hazırlık süresi uzundur.
- Donanım ve yazılımın yerleştirilmesi ve yapılandırılması zaman alabilir.

4. Mobil Siteler:

Tanım: Kriz anında kullanılmak üzere hazır durumda bekleyen ve taşınabilir bir şekilde tasarlanmış mobil ofisler veya veri merkezleridir.

Avantajları:

- Esneklik sağlar ve işletme ihtiyaçlarına göre yerleştirilebilir.

Dezavantajları:

- Lojistik zorluklar ve sınırlı kapasite.

5. Evden Çalışma (Remote Work):

Tanım: Çalışanların uzaktan çalışarak operasyonları sürdürdüğü bir modeldir.

Avantajları:

- Uygulaması genellikle düşük maliyetlidir.
- Özellikle pandemi gibi yaygın olaylar sırasında çok etkili bir çözüm sunar.

Dezavantajları:

- Evden çalışma için güvenli ve verimli bir IT altyapısının sağlanması gerekir.
- Fiziksel ekipman gereksinimi (örneğin, bilgisayar, internet erişimi).

Yedek Sistemler

Yedek sistemler, işletmenin kritik iş süreçlerini ve verilerini korumak ve bir arıza durumunda bunlara hızlı bir şekilde erişim sağlamak için geliştirilmiş teknolojik çözümlerdir.

Yedekleme Türleri:

1. **Veri Yedekleme:**
   - **Yerel Yedekleme:** Şirket içinde sunucular veya depolama cihazlarında yedekleme yapılır.
   - **Bulut Yedekleme:** Çevrim içi platformlar kullanılarak veriler güvenli bir şekilde yedeklenir.
   - **Hibrit Yedekleme:** Yerel ve bulut yedeklemenin bir arada kullanılması.

2. Sistem Yedekleme:

- **Replikasyon:** Sistemlerin birebir kopyalarının farklı bir yerde sürekli olarak güncellenmesi.
- **Snapshot (Anlık Görüntü):** Sistemlerin belirli bir andaki durumunun yedeğini alarak gerektiğinde bu duruma geri dönme imkanı.

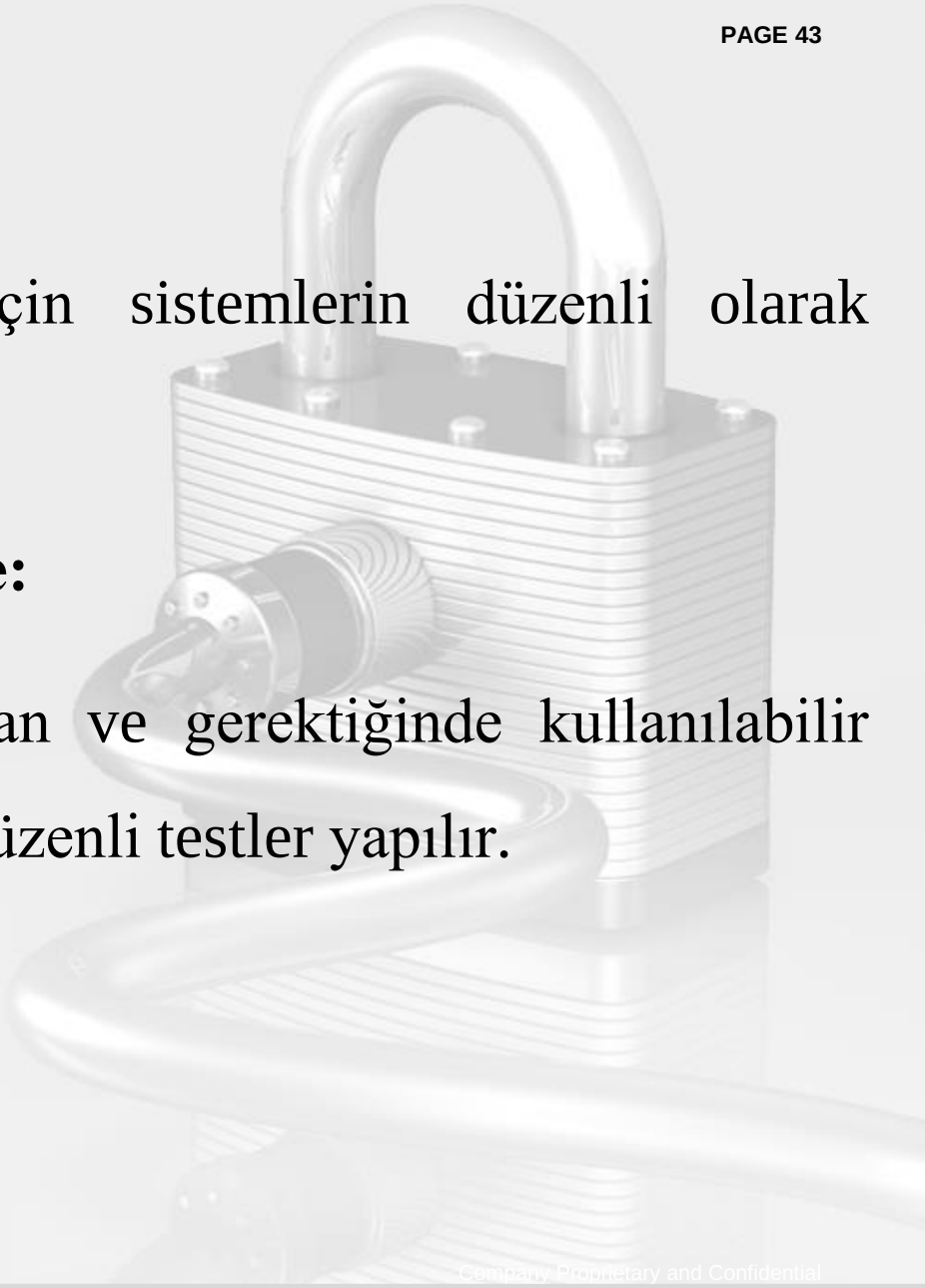
3. Ağ Yedekleme:

- Alternatif ağ altyapıları (örneğin, yedek internet sağlayıcılar) kullanılarak iletişim kesintilerinin önüne geçilir.

Örnek: Birincil bir ağ çökerse otomatik olarak yedek ağı devreye sokan SD-WAN teknolojileri.

Yedekleme Stratejileri:

1. **3-2-1 Kuralı:**
   - **3:** Üç farklı kopya oluşturun (orijinal veri + iki yedek).
   - **2:** Farklı iki ortamda yedekleme yapın (örneğin, yerel ve bulut).
   - **1:** Yedeklerden biri mutlaka farklı bir fiziksel lokasyonda bulunsun.
2. **RTO ve RPO Hedefleri:**
   - **Recovery Time Objective (RTO):** Sistemlerin veya verilerin ne kadar sürede yeniden çalışır hale getirileceği.
   - **Recovery Point Objective (RPO):** Verilerin kurtarılabileceği en son nokta (örneğin, son 1 saatlik veri kaybına izin verilebilir).



3. Otomatik Yedekleme:

- Manuel hataları önlemek için sistemlerin düzenli olarak otomatik yedekleme alması.

4. Düzenli Test ve Gözden Geçirme:

- Yedek sistemlerin çalıştığından ve gerektiğinde kullanılabilir olduğundan emin olmak için düzenli testler yapılır.

Alternatif Çalışma Yerleri ve Yedek Sistemlerin Birlikte Kullanımı

1. **Etkili Senkronizasyon:** Alternatif çalışma yerlerinde kullanılacak yedek sistemlerin sürekli olarak senkronize edilmesi, kesinti durumunda hızlı bir şekilde devreye alınmasını sağlar.

2. **Fiziksel ve Dijital Dayanıklılık:** Yedek sistemler, alternatif çalışma yerleriyle birlikte kullanıldığında hem fiziksel hem de dijital operasyonlar korunabilir.

3. **Esnek Çözümler:** İşletme ihtiyaçlarına göre en uygun alternatif yer ve yedek sistem kombinasyonu seçilir (örneğin, uzaktan çalışmayı destekleyen bulut yedekleme).

Özetle,

Alternatif Çalışma Yerleri ve Yedek Sistemler, bir kesinti durumunda işletmenin sürdürülebilirliğini ve hızla toparlanmasını sağlamak için vazgeçilmezdir.

İyi planlanmış ve düzenli olarak test edilmiş bu çözümler, işletmenin operasyonel dayanıklılığını artırır, mali kayıpları en aza indirir ve iş sürekliliği hedeflerine ulaşmasını sağlar

Eğitim

ve

Farkındalık

Eğitim ve Farkındalık, iş sürekliliği planlamasının (BCP) ve bilgi güvenliği yönetiminin (ISMS) temel bileşenlerinden biridir.

Amaç, çalışanların kriz durumlarında doğru adımları atmasını sağlamak, iş sürekliliği planlarını etkili bir şekilde uygulamak ve organizasyon genelinde bilinç oluşturup işletmeyi tehditlere karşı daha dayanıklı hale getirmektir.

Eğitim ve Farkındalık Neden Önemlidir?

- **Bilgi Eksikliğinin Giderilmesi:** Çalışanlar kriz durumunda nasıl hareket edeceklerini bilmiyorsa, en iyi planlar bile işe yaramayabilir.
- **Risklerin Azaltılması:** Eğitimli çalışanlar, hatalı davranışlardan kaynaklanabilecek riskleri azaltır.
- **Hızlı Tepki:** Acil durumlarda hız ve koordinasyonun sağlanmasına yardımcı olur.
- **Kültür Oluşturma:** İş sürekliliği ve güvenlik bilinci organizasyon kültürünün bir parçası haline gelir.
- **Yasal ve Düzenleyici Uyum:** Eğitim programları, yasal gerekliliklerin karşılanmasına ve uluslararası standartlara uyuma yardımcı olur (ör. ISO 22301, ISO 27001).

Eğitim ve Farkındalık Çalışmalarının Aşamaları

A. Eğitim İhtiyacının Belirlenmesi

1. **Risk Değerlendirmesi:** İşletmeye yönelik tehditler ve zafiyetler analiz edilerek eğitim gereksinimleri belirlenir.
2. **Hedef Kitle Analizi:**
   - Yönetim kadrosu, teknik ekip ve genel çalışanlar gibi farklı grupların farklı eğitim ihtiyaçları olabilir.
3. **Mevcut Bilgi Seviyesinin Ölçülmesi:** Çalışanların bilgi düzeyi değerlendirilir ve eksiklikler tespit edilir.

B. Eğitim Planlarının Hazırlanması

1. **Amaç ve Hedeflerin Tanımlanması:**
   - Örneğin, "çalışanların acil durum prosedürlerini öğrenmesi" veya "bilgi güvenliği farkındalığını artırmak."
2. **Kapsam ve Konuların Belirlenmesi:**
   - Acil durum yönetimi.
   - İş sürekliliği planlaması.
   - Siber güvenlik farkındalığı (ör. kimlik avı saldırıları, parola güvenliği).
3. **Eğitim Yöntemlerinin Seçimi:**
   - Sınıf eğitimleri, çevrim içi eğitimler, atölye çalışmaları, simülasyonlar.

C. Eğitim Materyallerinin Hazırlanması

1. **Kılavuzlar ve Rehberler:** İş sürekliliği planı, acil durum prosedürleri gibi dokümanlar hazırlanır.
2. **Senaryo Bazlı Çalışmalar:** Olası kriz senaryolarına dayalı uygulamalı eğitim içerikleri geliştirilir.
3. **Teknolojik Araçlar:** Çevrim içi eğitim platformları, video eğitimler, quizler.

D. Eğitim Programlarının Uygulanması

1. **Genel Eğitimler:**
   - Tüm çalışanlara yönelik temel farkındalık eğitimleri.
   - Örneğin, yangın tahliye prosedürleri, güvenli dosya paylaşımı.
2. **Özel Eğitimler:**
   - Kritik rollerdeki çalışanlara yönelik detaylı eğitimler.
   - Örneğin, IT ekiplerine yönelik sistem kurtarma eğitimi.
3. **Tatbikatlar:**
   - Gerçek senaryoları simüle ederek yapılan pratik eğitimler.
   - Örneğin, veri merkezi kesintisi veya deprem tahliyesi simülasyonu.

E. Eğitim Sonrası Değerlendirme

1. Katılım ve Performans Analizi:

- Eğitimlerin ne kadar etkili olduğunu anlamak için değerlendirme testleri ve geri bildirim anketleri yapılır.

2. Eksikliklerin Giderilmesi:

- Eğitimlerde eksik kalan noktalar belirlenir ve sonraki programlar buna göre düzenlenir.

Farkındalık Çalışmaları

Farkındalık, sürekli iletişim ve hatırlatma yoluyla çalışanların kritik konularda dikkatini yüksek tutmayı hedefler.

A. Farkındalık Araçları:

1. E-posta Kampanyaları:

- Düzenli bilgilendirme e-postalarıyla çalışanlara güvenlik ipuçları, prosedürler ve önemli hatırlatmalar gönderilir.
- Örnek: "Kimlik avı saldırılarına dikkat edin!" başlıklı uyarılar.

2. Poster ve Afişler:

- Ofis alanlarında kritik bilgi ve prosedürleri hatırlatan görseller.
- Örnek: "Yangın anında bu yolu kullanın."

3. Kısa Videolar:

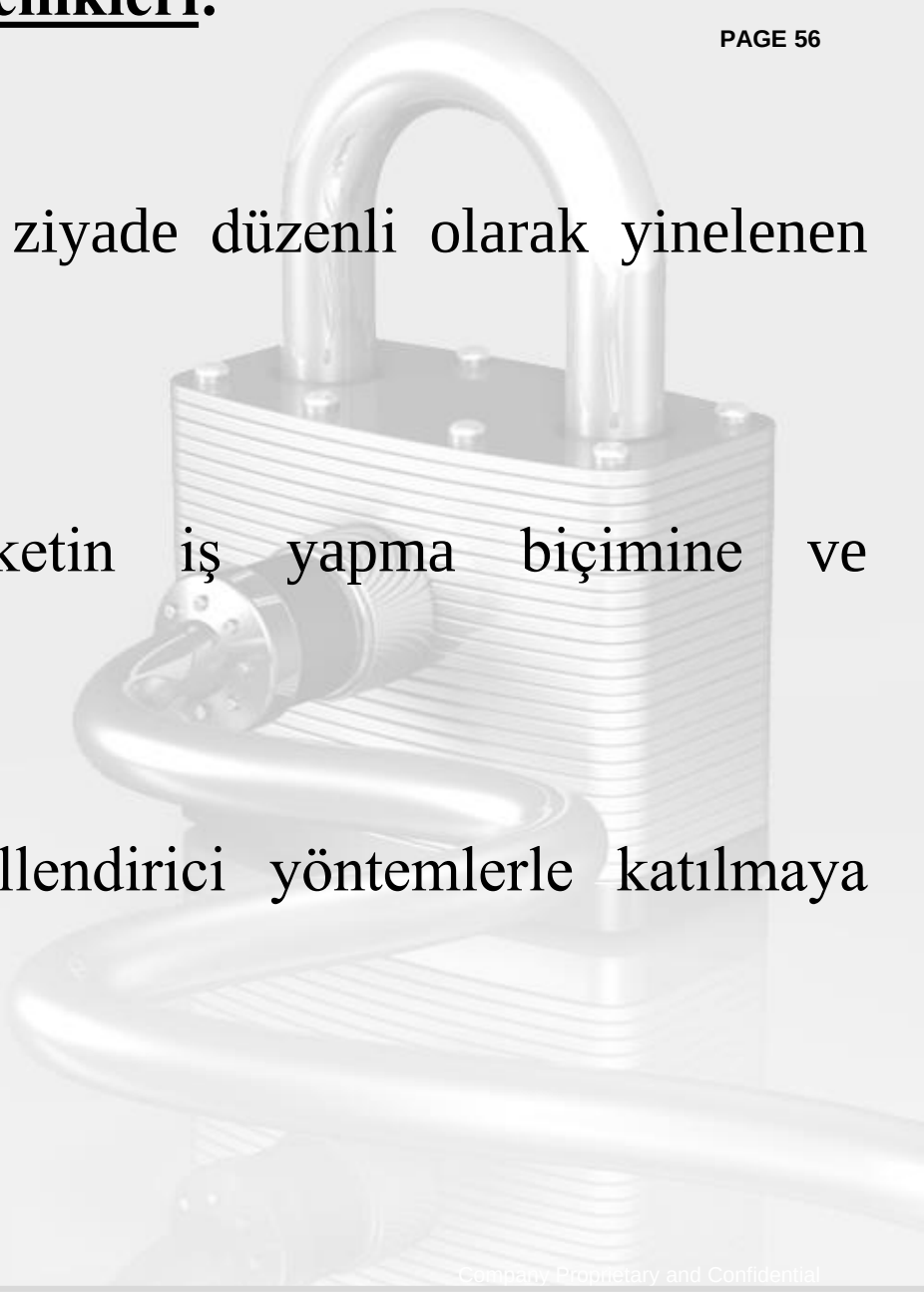
- Özellikle karmaşık süreçleri basit bir şekilde anlatan kısa ve etkili videolar.

4. Güvenlik Farkındalık Günleri:

- Şirket çapında farkındalık oluşturmak için etkinlikler düzenlenir.

B. Farkındalık Programlarının Özellikleri:

1. **Sürekli ve Tekrarlanan İletişim:**
   - Tek seferlik kampanyalardan ziyade düzenli olarak yinelenen programlar.
2. **Kültüre Uyum:**
   - Farkındalık çalışmaları, şirketin iş yapma biçimine ve değerlerine uygun olmalıdır.
3. **Motivasyon ve Katılım:**
   - Çalışanları eğlenceli ve ödüllendirici yöntemlerle katılmaya teşvik etmek.



Eğitim ve Farkındalık Konuları

- **Acil Durum Yönetimi:**

- Yangın, sel, deprem gibi doğal afetlerde ne yapılacağı.
- Tahliye prosedürleri.
- Acil durum ekipmanlarının (yangın söndürücüler, ilk yardım kitleri) kullanımı.

Bilgi Güvenliği:

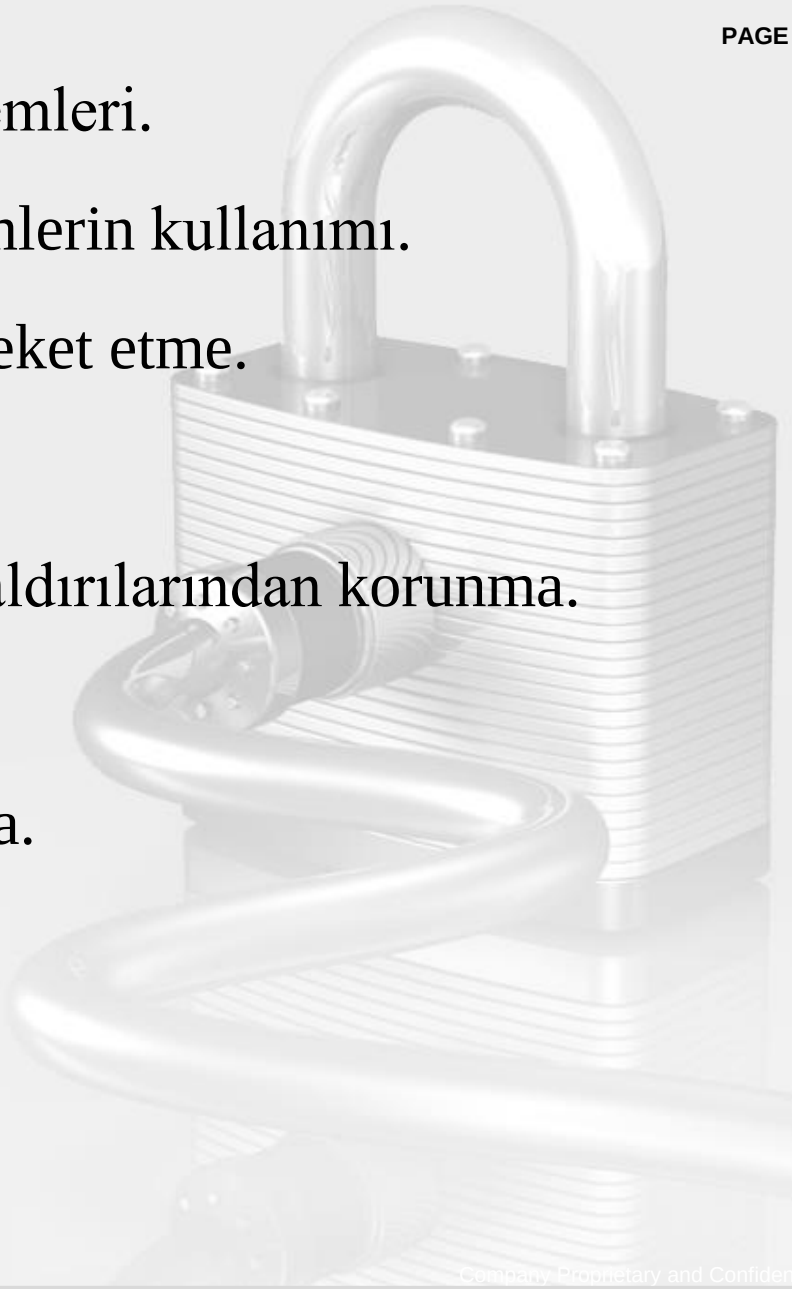
- Parola yönetimi ve iki faktörlü kimlik doğrulama.
- Kimlik avı saldırılarını tanıma ve önleme.
- Şüpheli e-postalar ve bağlantılarla başa çıkma.
- Çevrim içi veri paylaşımı ve şifreleme.

İş Sürekliliği Prosedürleri:

- Kritik süreçlerin toparlanma yöntemleri.
- Alternatif çalışma yerleri ve sistemlerin kullanımı.
- İş sürekliliği planlarına uygun hareket etme.

Siber Güvenlik Farkındalığı:

- Ransomware (fidye yazılımları) saldırılarından korunma.
- Güvenli internet erişimi.
- Şirket cihazlarını güvenli kullanma.



Eğitim ve Farkındalık Programlarının Başarısını Ölçmek

1. **Performans Değerlendirme:**
   - Eğitim sonrası çalışanların bilgi seviyesindeki artış ölçülür.
   - Örnek: Kimlik avı saldırı simülasyonlarına verilen tepkiler analiz edilir.
2. **Prosedürlere Uyumluluk:**
   - Çalışanların acil durum prosedürlerini ne kadar doğru uyguladıkları gözlemlenir.
3. **İşletme Performansı:**
   - Eğitim ve farkındalık çalışmaları sonrası, kesintiler sırasında hızlı toparlanma oranları değerlendirilir.

Özetle, Eğitim ve farkındalık, işletmelerin krizlere ve tehditlere karşı dayanıklılığını artırmanın temel yollarındandır.

Çalışanların bilgi düzeyini artırmak, farkındalıklarını yükseltmek ve bu bilgileri düzenli olarak güncellemek, işletmenin yalnızca kesintilere karşı değil, aynı zamanda itibar ve operasyonel kayıplara karşı da koruma sağlamasına yardımcı olur.