Küçük ve Orta Ölçekli İşletmeler (KOBİ'ler) için Siber Güvenliği

Talepler

VdS 3473tr : 2015-07 (01)

Editör ve Yayınevi: VdS Schadenverhütung GmbH

Amsterdamer Str. 172-174
D-50735 Köln
Telefon: (0221) 77 66 0; Fax: (0221) 77 66 341

Telif hakkı VdS Schadenverhütung GmbH aittir. Her hakkı mahfuzdur

Bilgi Güvenliği İçin VdS Direktifleri

Küçük ve Orta Ölçekli İşletmeler (KOBİ'ler) için Siber Güvenliği

Talepler

İçindekiler

1 Genel hususlar ... 6
1.1 Motivasyon ... 6
1.1 Geçerlilik alanı ... 6
1.2 Uygulama uyarıları ... 6
1.3 Geçerlilik ... 6
2 Normatif atıflar ... 6
3 Kavramlar ... 7
4 Bilgi Güvenliğinin Organizasyonu ... 11
4.1 Sorumluluklar ... 11
4.1.1 Eşleştirme Ve Dokümantasyon ... 11
4.1.2 Fonksiyonlar Ayrılığı ... 11
4.1.3 Kaynaklar ... 11
4.1.4 Görevlerin Devredilmesi ... 11
4.2 Üst yönetim ... 12
4.3 Bilgi Güvenliği Sorumlusu (BGS) ... 12
4.4 Bilgi Güvenliği Ekibi (BGE) ... 12
4.5 IT (BT) Sorumlusu ... 13
4.6 Sistem Yöneticileri ... 13
4.7 İnsan Kaynakları İle ilgili Sorumluluklara Sahip Olan Yöneticiler ... 13
4.8 Personel ... 13
4.9 Proje Sorumluları ... 13
4.10 Tedarikçiler Ve Diğer Görev (İş) Yüklenicileri ... 13
5 Bilgi Güvenliği İle İlgili Yönetmelik (BG Yönetmeliği) ... 14
5.1 Genel Talepler ... 14
5.2 Kapsam ... 14
6 Bilgi Güvenliği İle İlgili Yönergeler (BG Yönergeleri) ... 14
6.1 Genel Talepler ... 14
6.2 Kapsam ... 15
6.3 Kullanıcılar İçin Kurallar ... 15
6.4 Tedarikçiler Ve Diğer Görev (İş) Yüklenicileri İçin Kurallar ... 16
6.5 Diğer Kurallar ... 17
7 Personel ... 17
7.1 İşle Alımdan Önce ... 17
7.2 İşe Alım ve İş Başında Eğitim ... 17
7.3 İş Akdinin Sonlandırılması Veya Değiştirilmesi ... 18
8 Bilgi ... 18
8.1 Bilginin Güncelliği ... 18
8.2 Hassasiyet Oluşturmak, Temel ve İleri Eğitim ... 18

9 Kritik IT (BT) Kaynaklarının Belirlenmesi ... 19
9.1 Süreçler ... 19
9.2 Bilgiler ... 19
9.3 IT (BT) Sistemleri, Mobil Veri Taşıyıcıları ve Bağlantılar ... 19
9.4 Özgün Yazılımlar ... 20
10 IT (BT) Sistemleri ... 20
10.1 Envanter Listesi ... 20
10.2 Yaşam döngüsü ... 20
10.2.1 İşletime alım ve değiştirme ... 20
10.2.2 Kullanımdan Kaldırım Ve Yeniden Kullanım ... 21
10.3 Temel Koruma ... 21
10.3.1 Güncellemeler ... 21
10.3.2 Ağ Trafiğinin Sınırlandırılması ... 21
10.3.3 Raporlama ... 22
10.3.4 Harici Arabirimler Ve Sürücüler ... 22
10.3.5 Zararlı Yazılımlar ... 22
10.3.6 Yabancı Medyaların Başlatılması ... 22
10.3.7 Kimlik Doğrulama Süreci ... 22
10.3.8 Erişim Kısıtlamaları ... 23
10.4 Mobil IT (BT) Sistemleri İçin Ek Tedbirler ... 23
10.4.1 BG Yönergesi ... 23
10.4.2 Bilgilerin Korunması ... 24
10.4.3 Kayıp ... 24
10.5 Kritik IT (BT) Sistemleri İçin EK Tedbirler ... 24
10.5.1 Risk analizi Ve Risk Yönetimi ... 24
10.5.2 Acil Durum İşletim Seviyesi ... 24
10.5.3 Dayanıklılık ... 24
10.5.4 Harici Arabirimler Ve Sürücüler ... 25
10.5.5 Değişikliklerin Yönetilmesi ... 25
10.5.6 Dokümantasyon ... 25
10.5.7 Veri Yedekleme ... 25
10.5.8 Denetim ... 25
10.5.9 Yedek Sistemler ve Yöntemler ... 25
10.5.10 Kritik Özgün Yazılımlar ... 26
11 Ağlar ve Bağlantılar ... 26
11.1 Dokümantasyon ... 26
11.2 Aktif Ağ Bileşenleri ... 26
11.3 Ağ Geçitleri ... 26
11.4 Temel Koruma ... 26
11.4.1 Ağ Bağlantıları ... 27
11.4.2 Alt Bölümlere Ayırmak ... 27
11.4.3 Uzaktan Erişim ... 27
11.4.4 Ağların Birleştirilmesi ... 27
11.5 Kritik Bağlantılar İçin Ek Tedbirler ... 27
12 Mobil Veri Taşıyıcıları ... 28
12.1 BG Yönergesi ... 28
12.2 Kritik Mobil Veri Taşıyıcıları İçin Ek Tedbirler ... 28
12.2.1 Risk analizi Ve Risk Yönetimi ... 28
12.2.2 Kayıtlı Bilgilerin Korunması ... 28
12.2.3 Kayıplar ... 28

13 Ortam ... 28
13.1 Sunucular, Aktif Ağ Bileşenleri ve Ağ Dağıtım Noktaları ... 29
13.2 Veri Hatları ... 29
13.3 Kritik IT (BT) Sistemleri İçin EK Tedbirler ... 29
14 IT (BT) Outsourcing ve Cloud Computing ... 29
14.1 Hazırlık ... 29
14.2 Sözleşmenin Düzenlenmesi ... 30
14.3 Kritik IT (BT) Kaynakları İçin Ek Tedbirler ... 30
15 Girişler Ve Erişim Yetkileri ... 31
15.1 Yönetim ... 31
15.2 Kritik IT (BT) Sistemleri Ve Veriler İçin Ek Tedbirler ... 31
16 Veri Yedekleme Ve Arşivleme ... 32
16.1 BG Yönergesi ... 32
16.2 Arşivleme ... 32
16.3 Yöntem ... 32
16.4 Geliştirme ... 32
16.5 Temel Koruma ... 32
16.5.1 Depolama Yerleri ... 33
16.5.2 Sunucu ... 33
16.5.3 Aktif Ağ Bileşenleri ... 33
16.5.4 Mobil IT (BT) Sistemleri ... 33
16.5.5 Testler ... 33
16.6 Kritik IT (BT) Sistemleri İçin Ek Tedbirler ... 33
16.6.1 Risk Analizi ... 33
16.6.2 Yöntem ... 34
16.6.3 Testler ... 34
17 Arızalar ve Devre Dışı Kalma Durumları ... 34
17.1 BG Yönergesi ... 34
17.2 Reaksiyon ... 35
17.3 Kritik IT (BT) Sistemleri İçin Ek Tedbirler ... 35
17.3.1 Tekrar Çalıştırma Planları ... 35
17.3.2 Bağımlılıklar ... 35
18 Güvenlik İhlalleri ... 36
18.1 BG Yönergesi ... 36
18.2 Fark etmek ... 36
18.3 Reaksiyon ... 36
Ek A ... 37
A.1 Yöntem ... 37
A.2 Risk analizi Ve Risk Yönetimi ... 37
A.2.1 Risk Analizi ... 37
A.2.2 Risklerin Ele Alınması ... 37
A.2.3 Tekrarlanma ve Uyarlanma ... 38

1 Genel hususlar

1.1 Motivasyon

Bir işletmenin başarısı için sadece rekabete uygun ürünler ve hizmetler gerekli değildir. İşletmenin ticari, lojistik ve teknik iş süreçlerinin üstesinden gelmek için modern IT (BT) sistemlerinin kullanılması, ve bunun yanısıra internet bağlantısının olması, günümüzde dünya çapındaki rekabette varlığın sürdürülmesi için birer olmazsa olmazdır. Bununla birlikte dijitalleşme ve ağlara bağlılık, işletmelerin risk yönetimlerinde dikkate almak zorunda oldukları yeni tehlikeler de barındırmaktadır. İyi organize edilmiş bir bilgi güvenliği, zayıf noktaların adedini ve kalan riskleri azaltmaktadır ve bu sayede işletme için potansiyel hasarları sınırlandırmaktadır.

"Klasik" tehlikelerin bertaraf edilmesi için kendini kanıtlamış koruma standartları, özellikle de VdS Schadenverhütung GmbH şirketinin yönergeleri mevcuttur. Burada sunulan yönergeler ile VdS, uygun bir bilgi güvenliğinin yerleştirilmesi ve muhafaza edilmesi için özel olarak küçük ve orta ölçekli işletmeler (KOBİ'ler) için uyarlanmış bir yöntem geliştirmiştir.

1.1 Geçerlilik alanı

Bu yönerge, bilgi güvenliğine yönelik asgari talepleri belirlemektedir ve küçük ve orta ölçekli işletmeler (KOBİ'ler), esnaflar, idari birimler, birlik ve diğer organizasyonlar tarafından uygulanabilir.

1.2 Uygulama uyarıları

Burada sunulan yönergeler, VdS tarafından gerçekleştirilen sertifikalandırma sürecinin temelini oluşturmaktadır.

Talep edilen tedbirlerin uygulamaya konulması, bilgi güvenliği alanında uzmanlık bilgisi ve deneyim gerektirmektedir. Bu bilgiler yeterli ölçüde mevcut değil ise, VdS 3477 gereğince uygun yeterliliğe sahip bir hizmet sağlayıcısının görevlendirilmesini önermekteyiz.

1.3 Geçerlilik

Bu yönergeler 01.07.2015 tarihinden itibaren geçerlidir.

2 Normatif atıflar

Bu yönergeler, başka talimat ve direktiflere tarihli ve tarih içermeyen atıflar içermektedir. Atıflar ilgili bölümlerde yapılmaktadır, başlıklar aşağıda belirtilmiştir. Tarihli talimat ve yönergeler ile ilgili değişiklikler ve eklemeler, sadece burada sunulan yönergelerin değiştirilmesi ile bildirilmişlerse geçerlidir. Tarihsiz talimat ve yönergelerde, en son yayınlanan versiyon geçerlidir.

BSI-Standart 100-2 IT-Temel Koruma - Yöntemi

BSI-Standart 100-3 IT-Temel Korumasına göre Risk Analizi

BSI-Standart 100-4 Acil Durum Yönetimi

DIN EN 50173 Serisi Bilgi Teknolojisi – Uygulama Bakımından Nötr Kablo Sistemleri

DIN EN 50174-Serisi Bilgi Teknolojisi – Haberleşme Kablosu Sistemlerinin Kurulumu

DIN EN ISO 9001	Kalite Yönetim Sistemleri – Talepler
DIN EN ISO 22301	Kamu Güvenliği ve Kamunun Korunması – İş Sürekliliği Yönetim Sistemi (Business Continuity Management System) – Talepler
ISO 31000	Risk Yönetimi – Prensipler ve Kurallar
ISO/IEC 27005	Bilgi Teknolojileri – Güvenlik Teknikleri – Bilgi Güvenliği Risk Yönetimi
VdS 2007	Bilgi Teknolojisi Sistemleri (IT (BT) sistemleri) – Hasarların önlenmesine yönelik bilgi broşürü

3 Kavramlar

Yönetimsel giriş: Bir kullanıcıya bir IT sistemini yönetmeye olanak sağlayan giriştir, yani bir kullanıcıya bir IT (BT) sistemi içinde kapsamlı yetkiler sağlayan bir giriş olanağıdır.

Sistem Yöneticisi: Bir sistem yöneticisi, bir IT (BT) sisteminin veya ağ yapısının kurulumundan, işletilmesinden, denetiminden ve bakımından sorumludur.

Aktif ağ bileşenleri: Kendine ait bir mantığa sahip olan hub, switch, repeater, bridge, medya dönüştürücüsü, ağ geçidi, güvenlik duvarı vs. gibi ağ bileşenleridir. Aktif bir ağ bileşeni genelde bir güç kaynağına ihtiyaç duymaktadır. Aktif bir ağ bileşeni bir IT (BT) sistemidir.

Görev: Belirlenmiş eylemleri gerçekleştirmek üzere aktörlere iletilen sürekli etkili bir taleptir.

Aslına uygunluk: Gerçeklik, denetlenebilirlik ve güvenilirlik.

Aslına uygunluk özelliği: Sorgulayan merciin kimliğinizi kanıtlamak için kullanabileceği bir özellik. Kimlik doğrulama özellikleri, bir bilgi (örn. şifre veya PIN), sahip olunan bir obje (örn. çip kartı veya anahtarı) veya bir biometrik özellik (örn. parmak izi veya retina) olabilir.

Tehdit: Bir hasarın oluşması ile ilgili potansiyel bir ihtimaldir.

İş Sürekliliği Yönetimi (İSY = Business Continuity Management / BCM): Hedefi, ana iş süreçlerini acil durumlarda, krizlerde veya afetlerde dahi sürdürmek veya mümkün olduğu kadar hızlı bir şekilde yeniden başlatmak olan bütünsel bir yönetim sistemidir. Bu yönetim sistemi kapsamında hasar olayların üstesinden gelinmesi süreci, sistematik bir şekilde hazırlanmaktadır.

Bulut Bilişim: Konfigüre edilebilen IT (BT) kaynaklarından oluşan ortak bir havuza erişimi olanaklı hâle getiren bir teknolojidir.

Veriler: Bilinen mutabakatlar temelinde, bilgileri simgeleyen işaretlerden oluşan yapılardır.

Veri hattı: Veri alışverişine hizmet eden fiziksel bir medyadır.

Fonksiyon: İşletme hedefinin bir kısmının sağlanmasına hizmet eden bir görevler demetidir.

Tehlike: Korunacak bir objeye yönelik olası hasar etkisidir.

Potansiyel zarar kaynağı: Tehdit artı zayıf nokta.

Bilgi: Alıcının, aldığı verileri yorumlayarak çıkarttığı anlam ve önem.

Bilgi güvenliği: Mevcut güvenlik gereksinimleri bağlamında bilgilerin korunması (örn. gizlilik, kullanılabilirlik veya bütünlük).

Bilgi güvenliği sorumlusu (BGS): Bölüm 4.3 kapsamındaki görevleri gerçekleştiren kişi.

Bilgi güvenliği süreci: Bilgi güvenliğinin sağlanması, muhafaza edilmesi ve geliştirilmesi için gerekli etkinliklerin organizasyonel işleyişe entegrasyonu.

Bilgi güvenliği ekibi (BGE): Bölüm 4.4 kapsamındaki görevleri gerçekleştiren ekip.

Bilgi teknolojisi (IT): Bilgi ve veri işlenmesi ile birlikte veri aktarımı, ayrıca bunlar için gerekli donanımlar ve yazılımlar için kullanılan bir üst kavramdır.

Bütünlük: Bilgilerin doğruluğu (sağlamlığı) ve veri işlenme sürecinin doğru fonksiyon şeklidir.

BG Yönergesi: Bilgi güvenliği yönergesi; bkz. Bölüm 6.

IT (BT) alt yapısı: Uygulama yazılımlarının işletilmesi için maddi ve kurumsal türdeki tüm uzun ömürlü donanımlardır.

IT (BT) kaynağı: Elektronik bilgi işlenmesine hizmet eden kaynaklardır. Bunların arasında IT (BT) sistemleri, personel, veri taşıyıcıları, ayrıca veriler ve bilgiler bulunmaktadır.

IT (BT) sorumlusu: IT (BT) departmanının yöneticisi, veya bilgi teknolojisinden sorumlu olan yönetimdir.

IT-Outsourcing (BT için dış kaynaktan yararlanılması): IT (BT) görevlerinin hukuki açıdan bağımsız hizmet sağlayıcılarına devredilmesi.

IT (BT) sistemi: Bilgilerin işlenmesine hizmet eden ve kapalı bir fonksiyon birimi oluşturan teknik sistemlerdir. Tipik IT (BT) sistemleri örn. serverler (sunucular), client'ler (istemciler), yazıcılar, cep telefonları, akıllı telefonlar, telefon sistemleri, dizüstü bilgisayarlar, tablet bilgisayarlar ve aktif ağ bileşenleridir.

Afet niteliğinde hasarlar: Aşağıda belirtilen kriterlerden biri ile tanımlanabilen bir hasardır:

1. İnsanların sağlığına ve yaşamına yönelik etkiler:
   İnsanlar ağır yaralanmaktadır veya ölmektedir.
2. Ana iş süreçlerine yönelik etkiler:
   Ana iş süreçleri durmaktadır ve düzenli işleyişe geri dönülmesi (kabul edilebilir makul bir süre dâhilinde) mümkün değildir.
3. İşletmenin temel değerlerine yönelik etkiler:
   Temel işletme değerleri kaybolmaktadır veya zarar görmektedir ve bunların (işletmenin kaynakları ve olanakları kullanılarak) yeniden oluşturulması artık mümkün değildir.
4. Hukuki uygunluğa yönelik etkiler:
   Yasalar, sözleşmeler veya standartlar ihlal edilmektedir ve bu durumdan kaynaklanan hukuki sorumluluk işletme veya yetkililer için yıkıcıdır.
5. Hasar yüksekliği:
   Hasarın işletmenin kaynaklarıyla (imkanlarıyla) giderilmesi mümkün değildir.

Kritik IT (BT) sistemi: Bölüm 9.3 dâhilinde tanımlanan koşulları sağlayan IT (BT) sistemi.

Kritik mobil veri taşıyıcısı: Bölüm 9.3 dâhilinde belirtilen koşulları sağlayan mobil veri taşıyıcısı.

Kritik bağlantı: Bölüm 9.3 dâhilinde belirtilen koşulları sağlayan bağlantılar.

Yönetmelik: İşletmenin hedefini ve onun önceliğini tanımlayan, ayrıca hedefe erişmek için sorumlulukları belirleyen üst yönetimin yayınladığı bir belgedir.

Çalışan: İşletme ile bir sözleşme akdetmiş olan ve işletmede bir veya birden fazla pozisyona sahip olan gerçek kişidir.

Mobil Veri Taşıyıcıları: Kullanım amacında mobilitenin ön planda olduğu bir veri taşıyıcısıdır. Tipik mobil veri taşıyıcıları örn. flash bellekler ve hafıza kartları, harici sabit diskler, ayrıca CD-ROM, DVD ve disk gibi depolama medyalarıdır.

Mobil IT (BT) sistemi: Kullanım amacında mobilitenin ön planda olduğu bir IT (BT) sistemidir. Tipik mobil IT (BT) sistemleri örn. dizüstü bilgisayarlar, akıllı telefonlar, tablet bilgisayarlar veya dijital kameralardır.

Ağ bileşenleri: Verilerin iletilmesine hizmet eden teknik sistemlerdir. Ağ bileşenleri, aktif ve pasif ağ bileşenleri olmak üzere iki gruba ayrılmaktadır.

Ağ geçidi: İki farklı ağ yapısı arasındaki arabirimdir. Burada ağ yapıları fiziksel aktarım medyaları, kullanılan protokoller veya farklı yönetimsel hiyerarşiler bakımından birbirinden farklı olabilir.

Acil Durum İşletim Seviyesi: Bir IT (BT) sisteminden, bir acil durum işletiminin muhafaza edilmesinin mümkün olması için sağlanacak olan fonksiyonların tanımıdır.

Acil durum: Bir işletmenin süreçlerinin veya kaynaklarının öngörüldüğü gibi işlevsel olmadığı durumdur. Bu durum nedeniyle oluşan hasarlar, kabul edilebilir sınırın üzerindedir. Bir acil durum, genel günlük işleyiş dâhilinde ele alınamaz.

Pasif ağ bileşeni: Kendine ait bir mantığı olmayan ağ bileşeni, örn. kablo, bağlantı paneli, priz, soket, fiş vs. Pasif bir ağ bileşeni genelde bir güç kaynağına ihtiyaç duymaz.

Personel: Dâhili ve harici çalışanlardır.

Fiziksel erişim: Fiziksel bir şekilde bir IT (BT) sistemi veya bir ağ ile etkileşime girmeye olanak sağlayan durum veya koşuldur.

Pozisyon: Bir işletmenin hiyerarşisi içinde çalışanın aldığı konumu tanımlamaktadır.

Proje sorumlusu: İşletmenin bir projesinin kurallara uygun şekilde gerçekleştirilmesinden sorumlu olan kişidir.

Süreç: Araçlar yardımıyla girdileri sonuçlara dönüştüren bir faaliyetler sistemidir.

Yüksek hasar potansiyeli olan süreç: Hatalı işleyişte veya kısa süreli devre dışı kaldığında vahim hasarlara neden olan bir süreçtir.

Süreç sorumlusu: İçerik bakımından bir veya birden fazla iş sürecinden sorumlu olan kişidir. Bu kişi bu iş süreci için gerekli olan kaynaklar ve kendisine yönelik talepler ile ilgili genel bir bakışa sahiptir.

Kaynak: İşletmeye ait olan veya onun hizmetinde olan işletim maddeleri ve araçlarıdır.

Risk: Ortaya çıkma olasılığı ve hasar yüksekliği temelinde değerlendirilmiş olan bir 'potansiyel zarar kaynağıdır'.

Rol: Bir pozisyona yönelik tutum beklentileri ve sorumluluklar demetidir.

Arabirim: IT (BT) sisteminin haberleşmeye hizmet eden bölümüdür. Bu kapsama sadece Ethernet veya kablosuz ağ adaptörleri girmez. Bu kapsama ayrıca ISDN kartı, modemler, USB portları, NFC ve kızılötesi arabirimleri, SD-Slot'ları ve klavye gibi bileşenler girmektedir.

Zayıf nokta: Bir tehdidin, korunması gerekli olan bir obje ile mekânsal ve/veya zamansal olarak bir araya gelmesine olanak sağlayan bir durumdur.

Sunucu: Fonksiyonel ve alt yapısal ağ hizmetlerinin gerçekleştirilmesine hizmet eden merkezi bir IT (BT) sistemidir.

Güvenlik ihlali: Bilgi güvenliğine etki eden ve sonucunda hasarların ortaya çıkabileceği istenmedik bir olaydır. Bir güvenlik ihlali olarak tam olarak neyin veya nelerin değerlendirileceği, özgün şekilde her işletmenin kendisi tarafından tanımlanmalıdır.

Arıza: Bir işletmenin süreçlerinin veya kaynaklarının öngörüldüğü gibi işlevsel olmadığı durumdur. Bu durumun neden olduğu hasarlar, düşük olarak sınıflandırılabilir. Arızanın giderilmesi işi, genel günlük işleyiş dâhilinde gerçekleştirilebilir.

Sistem yazılımı: Donanım yazılımları, işletim sistemleri ve sisteme bağlı yazılımlardır. Sistem yazılımları bir IT (BT) sisteminin dâhili ve harici donanım bileşenlerini yönetmektedir.

Üst yönetim: Yönetim kurulu başkanı ve üyeleri, genel müdürler veya kamu kurumu yöneticileri gibi üst yönetim kademeleridir.

Bağlantı: Veri alışverişinin gerçekleştirildiği kanaldır.

Yöntem: Bir sürecin (veya bir süreç dâhilindeki münferit faaliyetin) ne şekilde ve türde uygulanacağını belirleyen kurallar bütünüdür.

Kullanılabilirlik: Bir sistemin belirli talepleri, üzerinde mutabakat sağlanan bir zaman çerçevesi dâhilinde gerçekleştirmesi olasılığıdır. Bilgilerin kullanılabilirliği, bunlar her zaman öngörüldüğü şekilde kullanılabilirse sağlanmıştır.

Gizlilik: Bir haberin sadece kısıtlı bir alıcı topluluğu için öngörülmüş olması özelliğidir. Bilgilerin gizliliği, sadece bunlar için öngörülen alıcı topluluğu bunları okuyabiliyor veya yorumlayabiliyor ise sağlanmıştır.

Ana iş süreci: İşletmenin görevlerini yerine getirmesi için belirleyici bir öneme sahip olan iş sürecidir. Bu örn. bir değer yaratma süreci veya rekabet kabiliyetinin muhafaza edilmesi veya iyileştirilmesi için bir süreç olabilir.

Giriş: İşletmeye ait kamuya açık olmayan IT (BT) alt yapısı ile haberleşmeye olanak sağlayan düzendir (donanımdır).

Erişim: Erişimi gerçekleştiren bir mercii ve bir IT (BT) sistemi arasındaki veri alışverişidir.

4 Bilgi Güvenliğinin Organizasyonu

Bilgi güvenliği dinamiktir ve her işletme için özgün yapıdadır. İşletme tarafından hedeflenen güvenlik seviyesini mümkün olduğunca az zahmetle ve düşük maliyetle tanımlamak, uygulamak ve sürekli şekilde güncel ihtiyaçlara ve potansiyel zarar kaynaklarının durumuna uyarlamak için, uygun bir sürecin (bilgi güvenliği sürecinin) uygulamaya konulması gereklidir.

4.1 Sorumluluklar

Bilgi güvenliği süreci için sorumluluklar anlaşılır ve çelişkisiz şekilde ilgililere EŞLEŞTİRİLMELİDİR.

4.1.1 Eşleştirme Ve Dokümantasyon

Bilgi güvenliği süreci dâhilinde her sorumluluk için yazılı bir şekilde aşağıda belirtilen hususlar KAYDEDİLMELİDİR:

1. Erişilmesi amaçlanan hedefler
2. Sorumluluk hangi kaynaklar için geçerli
3. Hedeflere erişmek için hangi görevler yerine getirilmelidir
4. Sorumluluğa, bu sorumluluğun yerine getirilmesi için hangi yetkiler ilişkilendirildi
5. Sorumluluğun yerine getirilmesi için hangi kaynaklar kullanımdadır veya hizmettedir
6. Sorumluluğun yerine getirilmesi hangi pozisyon(lar) tarafından kontrol ediliyor
7. Sorumluluğu hangi pozisyonlar yerine getirecek

4.1.2 Fonksiyonlar Ayrılığı

Bilgi güvenliği süreci dâhilindeki sorumlulukların dağıtımında fonksiyonlar ayrılığı prensibi UYGULANMALIDIR. Çelişkili sorumluluklar kesinlikle tek bir kişi veya işletme birimleri tarafından yerine GETİRİLMEMELİDİR.

Fonksiyonlar ayrılığı mümkün değilse veya sadece kabul edilemez yüksek zahmet ve/veya maliyetle mümkün ise, faaliyet denetimi, kontroller veya performans denetimi gibi başka tedbirler UYGULAMAYA KONULMALIDIR.

Fonksiyonlar ayrılığı mümkün değil ise, bu durum dokümantasyondaki fonksiyonların dağılımı ile ilgili kısımda özellikle BELİRTİLMELİDİR ve nedenler AÇIKLANMALIDIR.

Bilgi güvenliği sürecinde sorumlulukların kesişmesinin veya sorumluluk boşluklarının önlenmesi için, ilgili kurallar yılda bir kere bilgi güvenliği sorumlusu (BGS) tarafından KONTROL EDİLMELİDİR.

4.1.3 Kaynaklar

Bilgi güvenliği süreci dâhilindeki sorumlulukların yerine getirilmesi için, ilgili personel gerekli kapsamda (bkz. Bölüm 4.1.1) diğer faaliyetlerinden MUAF TUTULMALIDIR.

4.1.4 Görevlerin Devredilmesi

Bilgi güvenliği sorumluları görevlerini başka kişilere DEVREDEBİLİR. Ancak sorumluluk kendilerine kalmaktadır. Bu nedenle devrettikleri görevlerin yerine getirilip getirilmediğini ve sonucu KONTROL ETMEK ZORUNDADIRLAR.

4.2 Üst yönetim

Üst yönetim, aşağıda belirtilen sorumlulukları yerine getireceğini TAAHHÜT ETMELİDİR:

1. Bilgi güvenliği için bütün sorumluluğu üstlenmek
2. Bilgi güvenliği süreci için sorumluluğu üstlenmek
3. Bilgi güvenliği için yönergeleri yürürlüğe koymak (BG Yönergeleri)
4. Bilgi güvenliği için gerekli teknik ve maddi kaynakları, ayrıca gerekli personeli hazır bulundurmak
5. Bilgi güvenliğini işletmenin iç yapısı, hiyerarşileri ve iş süreçleri içine entegre etmek

4.3 Bilgi Güvenliği Sorumlusu (BGS)

Üst yönetim, bir bilgi güvenliği sorumlusunun (BGS) sorumluluklarını bir çalışana atamakla YÜKÜMLÜDÜR.

Bu kişi aşağıda belirtilen sorumlulukları yerine getirmek ZORUNDADIR:

1. Bilgi güvenliği süreci başlatmak, planlamak ve yönetmek
2. Somut iyileştirme önerileri geliştirmek
3. BG yönetmeliğini oluştururken, ayrıca yıllık denetimlerde ve BG yönetmeliğinin uyarlanmasında üst yönetime destek sağlamak (bkz. Bölüm 2)
4. Bilgi güvenliği ile ilgili önemli konularda üst yönetime destek sağlamak
5. Tüm BG yönergelerini oluşturmak, yıllık olarak denetlemek ve uyarlamak
6. Güvenlikle ilgili olayları incelemek
7. Farkındalık yaratılmasına ve eğitime yönelik tedbirleri oluşturmak, uygulamaya koymak ve yönetmek
8. Bilgi işleme etkisi olan projelerde, ayrıca yeni yazılımların ve IT (BT) sistemlerinin hizmete alınmasında iletişim kurulacak kişi olmak ve bu şekilde güvenlikle ilgili hususların yeterince dikkate alındığını garanti etmek
9. Bilgi güvenliği ekibine (BGE) yıllık dönemlerde işletmedeki bilgi güvenliğinin güncel durumu, özellikle de riskler ve güvenlik ihlalleri hakkında rapor sunmak
10. Bilgi güvenliği konusunda iletişim kurulacak yetkili kişi rolünü yerine getirmek

4.4 Bilgi Güvenliği Ekibi (BGE)

Üst yönetim bir bilgi güvenliği ekibini (BGE) görevlendirmek ZORUNDADIR.

Bu ekipte aşağıda belirtilen işletme birimleri veya pozisyonları şahsen veya temsilciler üzerinden TEMSİL EDİLMİŞ DURUMDA OLMALIDIR:

1. Üst yönetim
2. BGS
3. IT (BT) Sorumlusu
4. Personel
5. Veri güvenliği sorumlusu (şayet mevcut ise)
6. Ekip, BGS'yi aşağıda belirtilen faaliyetlerde DESTEKLEMEK ZORUNDADIR:

7. BG Yönetmeliğinin ve tüm BG yönergelerinin oluşturulması
8. BG Yönetmeliğinin ve tüm BG yönergelerinin yıllık olarak kontrol edilmesi
9. İşletme çapında bilgi güvenliği tedbirlerinin koordine edilmesi ve yönetilmesi
10. Yeni potansiyel zarar kaynaklarının tespit edilmesi

4.5 IT (BT) Sorumlusu

Bir IT (BT) sorumlusunun görevleri üst yönetim tarafından bir çalışana ATANMALIDIR.

IT sorumluları aşağıda belirtilen görevleri YERİNE GETİRMEK ZORUNDADIR:

1. Sorumluluk alanı dâhilinde BG yönergelerinin uygun teknik ve organizasyonel tedbirlerle uygulanması sağlamak
2. Sorumluluk alanları dahilindeki bilgi güvenliğini iyileştirici ve koruyucu tüm tedbirler konusunda BGS ile teyitleşmek ve bunların planlanması, koordine edilmesi ve uygulamaya konulması

4.6 Sistem Yöneticileri

Bir sistem yöneticisinin sorumlulukları en az bir çalışana ATANMALIDIR.

Sistem yöneticileri aşağıda belirtilen sorumlulukları yerine getirmek ZORUNDADIR:

1. Bilgi güvenliği sürecine, IT (BT) sorumlusu ile mutabakat sağlayarak teknik tedbirleri entegre etmek
2. Bilgi güvenliğinin iyileştirilmesi için öneriler geliştirmek

4.7 İnsan Kaynakları İle ilgili Sorumluluklara Sahip Olan Yöneticiler

İnsan kaynakları ile ilgili sorumluluklara sahip olan yöneticiler, bilgi güvenliği ile ilgili teknik ve organizasyonel tedbirlerin alt kadrolarında bulunan personel tarafından uygulandığını GARANTİ ETMEK ZORUNDADIR.

4.8 Personel

Personel aşağıda belirtilen görevleri YERİNE GETİRMEK ZORUNDADIR:

1. Bilgi güvenliği kapsamında kendileri veya faaliyetleri ile ilgili olan tüm tedbirleri, kural ve düzenlemeleri uygulamak ve tümüne uymak
2. Arızaları, güvenlik ihlallerini ve acil durumları bildirmek

4.9 Proje Sorumluları

Proje sorumluları, BGS'suna bilgi işleme etkisi olan tüm projelerde, güvenlik ile ilgili hususların yeterli şekilde dikkate alındığını garanti etmek için DANIŞMAK ZORUNDADIR.

4.10 Tedarikçiler Ve Diğer Görev (İş) Yüklenicileri

İşletme, tedarikçileri ve diğer görev (iş) yüklenicilerinden - şayet bunlar kritik bilgilere (bkz. Bölüm 9.2) erişim yetkisine sahip iseler veya bilgi teknolojisinin (BT) kamuya açık olmayan alanlarını kullanıyorlarsa - kendileri ile ilgili bilgi güvenliğini ilgilendiren tedbir, kural ve düzenlemeleri uygulama ve tümüne uyma konusunda bir taahhüt almalıdır.

5 Bilgi Güvenliği İle İlgili Yönetmelik (BG Yönetmeliği)

Bilgi güvenliği ile ilgili yönetmelik (BG Yönetmeliği) tüm bilgi güvenliği sürecinin esasını oluşturan temel dokümandır. Bu doküman içerisinde üst yönetim tarafından sorumluluklar ve yetkiler, ayrıca erişilmesi istenen hedefler tanımlanmaktadır.

5.1 Genel Talepler

BG yönetmeliği, üst yönetim tarafından karara bağlanmalıdır ve ilan edilmelidir.

Üst yönetim, BG yönetmeliğini yıllık dönemlerle güncellik konusunda kontrol ettirmek ve gerekli ise bir güncelleştirilmesini sağlamak ZORUNDADIR.

BG yönetmeliği, her güncellemeden sonra zaman kaybedilmeden YAYINLANMALIDIR ve ilgili güncel hâli ile personelin hizmetine sunulmalıdır.

5.2 Kapsam

BG yönetmeliği, aşağıda belirtilen talepleri ve özellikleri SAĞLAMAK ZORUNDADIR:

1. İşletme dâhilinde bilgi güvenliğin hedeflerini ve önemini tanımlamak.
2. Bilgi güvenliği süreci için tüm pozisyonları tanımlamak ve bunların görevlerini açıklamak.
3. Uyulmaması durumundaki sonuçlara dikkat çekmek.

6 Bilgi Güvenliği İle İlgili Yönergeler (BG Yönergeleri)

BG yönetmeliğinin desteklenmesi ve somutlaştırılması kapsamında, bilgi güvenliği için daha ayrıntılı kuralların yürürlüğe konulması gereklidir. Bunlar BG yönergeleri olarak adlandırılan münferit dokümanlar dâhlinde bir araya getirilmelidir.

6.1 Genel Talepler

Her BG yönergesi, BGS tarafından BGE ile işbirliği yapılarak oluşturulmalıdır ve üst yönetim tarafından YÜRÜRLÜĞE KONULMALIDIR.

BGS, her BG yönergesini yıllık dönemlerle güncellik konusunda kontrol etmek ve gerekli olması hâlinde güncelleştirmek ZORUNDADIR.

BG yönergelerinin oluşturulması ve uyarlanması esnasında tüm yasal, kamu kurum ve kuruluşları tarafından uygulamaya konulan ve sözleşmelerle tanımlanan gerekler BELİRLENMELİDİR ve uygun şekilde UYGULAMAYA KONULMALIDIR.

BG yönergeleri, her güncelleme işleminden sonra hedef gruplarına zaman kaybedilmeden BİLDİRİLMELİDİR.

Bu işlem, hedef grup için erişilebilir ve anlaşılabilir bir şekilde GERÇEKLEŞMELİDİR, örn. bir eğitim faaliyet kapsamında.

BG yönergelerinin işletme dâhlinde uygulanması ZORUNLUDUR veya bunlar üst yönetim tarafından yürürlükten kaldırılmalıdır.

6.2 Kapsam

Her BG yönergesi, aşağıda belirtilen talepleri ve özellikleri SAĞLAMAK ZORUNDADIR:

1. Kim için bağlayıcı olduğu bilgisini içermek.
2. Neden oluşturulduğunun gerekçesini ve neyin hedeflendiğinin bilgisini içermek.
3. BG yönetmeliğini veya başka yönergelerini ihlal etmemek.
4. Uyulmaması durumundaki sonuçlara dikkat çekmek.

6.3 Kullanıcılar İçin Kurallar

IT'nin (BT'nin) kullanılması için kurallar TANIMLANMALIDIR. Bunlar tüm kullanıcılar (yönetim kademeleri dâhil) ve komple IT (BT) sistemi için bağlayıcı olmalıdır.

Aşağıda belirtilen kurallar OLUŞTURULMALIDIR:

1. Genel kullanım koşulları
   a. Telif hakları ile koruma altında olan içeriklerin yetkisiz şekilde çağrılması veya yayınlanması yasaklanmalıdır.
   b. Ceza kanunlarının konusu olan veya ahlak kurallarına uygun olmayan içeriklerin çağrılması veya yayınlanması yasaklanmalıdır.
2. Kişisel özel kullanım
   a. IT (BT) ile ilgili olarak kişisel özel kullanıma izin verilip verilmediği tanımlanmalıdır.
   b. Şayet IT (BT) için kişisel özel kullanıma izin veriliyorsa, IT (BT) işletme tarafından uygun şekilde düzenlenmelidir.
3. Temel davranış kuralları
   a. Sadece onaylı donanım ve yazılım IT (BT) alt yapısına kurulmalı, kullanılmalı veya işletilmelidir.
   b. Özgün, kişisel ağ geçitlerinin kurulması yasaklanmalıdır; istisnasız şekilde sadece işletme tarafından hizmete sunulan ağ geçitlerinin kullanımı onaylanmalıdır.
   c. IT (BT) alt yapısına kurulan güvenlik donanımları sökülmemeli, devre dışı bırakılmamalı, kötü niyetle kullanılmamalı veya bunlara ait konfigürasyon değiştirilmemelidir.
   d. Giriş bilgileri (tanımlamaları) üçüncü kişilere aktarılmamalıdır.
   e. Bilgiler yetkisiz şifrelenemez veya okuma erişiminden korunamaz; bunun için sadece işletme tarafından özel olarak bu işlem için onaylanmış olan teknik yöntemler kullanılmalıdır.
4. Kişi yerinde değilse bilgi akışı
   a. Yerine olmayan bir kullanıcı için yeni gelen mesajların başkalarına iletilip iletilmeyeceği hususu düzenlenmelidir.
   b. Yerinde olmayan kullanıcının veri deposuna ne zaman ve hangi koşullarda erişim sağlanacağı hususu düzenlenmelidir.
5. Kötü amaçlı kullanıma yönelik kontrol
   a. Kötü amaçlı kullanıma yönelik kontroller için mekanizmalar tanımlanmalı ve ilgililere bildirilmelidir.

İşletme, yukarıda belirtilen kural ve düzenlemeler için özel gerekçelere sahip durumlarda istisnalara OLANAK SAĞLAMALIDIR.

İstisnalar, BGS tarafından önceden ONAYLANMALIDIR ve gerekçelerle birlikte bir rapor içerisinde BELGELENDİRİLMELİDİR.

6.4 Tedarikçiler Ve Diğer Görev (İş) Yüklenicileri İçin Kurallar

IT'nin (BT'nin) kamuya açık olmayan alanlarını veya işletmeye ait IT (BT) alt yapısını kullanan tüm tedarikçiler ve diğer görev (iş) yüklenicileri için bağlayıcı olan kurallar YÜRÜRLÜĞE KONULMALIDIR.

Aşağıda belirtilen kurallar OLUŞTURULMALIDIR:

1. Genel kullanım koşulları
   a. Telif hakları ile koruma altında olan içeriklerin yetkisiz şekilde çağrılması veya yayınlanması yasaklanmalıdır.
   b. Ceza kanunlarının konusu olan veya ahlak kurallarına uygun olmayan içeriklerin çağrılması veya yayınlanması yasaklanmalıdır.
2. Kişisel özel kullanım
   a. IT'nin (BT'nin) özel şekilde kişisel kullanımı yasaklanmalıdır.
3. Temel davranış kuralları
   a. Güvenlik donanımlarındaki değişiklikler, ayrıca ağ geçitlerinin (örn. bakım için yapılan uzaktan erişimler veya VPN bağlantıları) kurulması için önceden BGS ile mutabakat sağlanmalıdır.
   b. Giriş bilgilerinin (tanımlamalarının) üçüncü kişilere aktarılması yasaklanmalıdır.
   c. Bilgilerin onay alınmadan şifrelenmesi veya okuma erişiminden korunması yasaklanmalıdır; bunun için sadece işletme tarafından özel olarak bu işlem için onaylanmış olan teknik yöntemler kullanılmalıdır.
4. Kamuya açık olmayan IT'ye (BT'ye) erişim
   a. Kamuya açık olmayan IT'ye (BT'ye) erişimler için önceden BGS ile mutabakat sağlanmalıdır.
   b. Şayet hizmet sağlayıcısının IT (BT) sistemleri kamuya açık olmayan IT'ye (BT'ye) erişiyorsa, bunlar temel güvenlik tedbirleri üzerinden güvenceye alınmalıdır; bunun için işletme minimum gereksinimleri tanımlanmalıdır.
5. IT (BT) sistemlerinin entegre edilmesi
   a. Bir IT (BT) sistemi işletmeye ait IT (BT) alt yapısına entegre edilmeden önce, bu sistem bir sistem yöneticisi tarafından onaylanmalıdır.
6. İşletmeye ait verilerin kullanılması
   a. Prensip olarak işletmeye ait veriler, işletmenin IT (BT) alt yapısı içinde kalmalıdır ve yabancı IT (BT) sistemlerine veya veri taşıyıcılarına aktarılmaları yasaktır.
   b. Mobil veri taşıyıcıların kullanımı için önceden ilgili sistem yöneticisi tarafından onay alınmalıdır.
   c. Mobil veri taşıyıcıları IT içinde kullanılmadan önce zararlı yazılımlar konusunda test edilmelidir, ancak bundan sonra IT (BT) içinde kullanılırlar.
   d. İşletmeye ait verilerin kayıtlı olduğu veri taşıyıcıları, her zaman gizlilik ilkelerine uygun şekilde kullanılmalıdır; bunlar üçüncü kişilere verilmez veya başka kişilerin erişimine açık şekilde muhafaza edilmez.
7. Kötü amaçlı kullanıma yönelik kontrol
   e. Kötü amaçlı kullanıma yönelik kontroller için mekanizmalar tanımlanmalı ve ilgililere bildirilmelidir.

İşletme, yukarıda belirtilen kural ve düzenlemeler için özel gerekçelere sahip durumlarda istisnalara OLANAK SAĞLAMALIDIR.

İstisnalar, BGS tarafından ONAYLANMALIDIR ve gerekçelerle birlikte bir rapor içerisinde BELGELENDİRİLMELİDİR.

6.5 Diğer Kurallar

Bu VdS direktifleri çerçevesinde daha ayrıntılı konulara özgün BG yönergeleri oluşturulmalıdır:

1. Mobil IT sistemleri (bkz. Bölüm 10.4)
2. Mobil veri taşıyıcısı (bkz. Bölüm 12.1)
3. Veri Yedekleme (bkz. Bölüm 16.1)
4. Hatalar ve devre dışı kalma durumları (bkz. Bölüm 17.1)
5. Güvenlik durumları (bkz. Bölüm 18.1)

Daha kapsamlı BG yönergeleri için ihtiyaç olup olmadığı yıllık olarak BGS tarafından BELİRLENMELİDİR.

7 Personel

Personel, bilgi güvenliğinin hayata geçirilmesi ve muhafaza edilmesi için temel bir etmendir. Bu nedenle insan kaynakları yönetiminde de bilgi güvenliği ile ilgili gereklerin dikkate alınması gereklidir.

7.1 İşle Alımdan Önce

İşletmenin bilgi güvenliği için önemli bir pozisyona bir kişi işe alınacaksa, işletme adayın gerekli uygunluğa ve güvenilirliğe sahip olmasını GARANTİ ETMEK ZORUNDADIR.

7.2 İşe Alım ve İş Başında Eğitim

İşe alım ve iş başında eğitim kapsamında, aşağıda belirtilen hususları garanti eden bir yöntem (bkz. Ek A 1) OLUŞTURULMALIDIR ve ENTEGRE EDİLMELİDİR:

1. İşe alınan kişi bir 'Gizlilik Beyanı" imzalamalıdır, bu beyan iş akdinin sona erdirilmesinden veya değiştirilmesinden sonra da yürürlükte kalan bilgi güvenliği ile ilgili yükümlülükleri tanımlamalıdır.
2. Yeni personel BG yönetmeliği, tüm bağlayıcı olan BG yönergeleri ve bilgi güvenliği ile ilgili diğer bağlayıcı kural ve düzenlemeler konusunda eğitilmelidir.
3. Yeni personel, kendileri için önemli güvenlik mekanizmalarının kullanımı konusunda eğitilmelidir (bkz. Bölüm 8.2).
4. Yeni personele gerekli olan giriş ve erişim yetkileri teslim edilir (bkz. Bölüm 15) ve personel bunların kullanımı konusunda eğitilir.

7.3 İş Akdinin Sonlandırılması Veya Değiştirilmesi

1. İş akdinin sonlandırılmasından veya değiştirilmesinden sonra aşağıda belirtilen hususları garanti eden bir yöntem (bkz. Ek A 1) OLUŞTURULMALIDIR ve ENTEGRE EDİLMELİDİR:
2. Şayet gerekli ise personel, müşteriler, tedarikçiler ve diğer görev (iş) yüklenicileri personel ve işletmedeki değişiklikler konusunda bilgilendirilir.
3. Çalışanın girişleri ve erişim yetkileri (bkz. Bölüm 15) derhal kontrol edilir ve gerektiği takdirde uyarlanır.

8 Bilgi

Çok sayıda potansiyel zarar kaynakları bilgisizlikten veya sorunlar konusunda yetersiz bilinçlilik nedeniyle oluşmaktadır veya en azından bu etkenler tarafından güçlendirilmektedir. Bu nedenle işletmenin bilgi güvenliği konusunda güncel bilgiye sahip olması, personelin sorumluluklarını anlamış olması ve personelin görevleri için uygun, ayrıca yeterli mesleki eğitime sahip olması gereklidir.

8.1 Bilginin Güncelliği

İşletmenin tüm ilgili noktalarının, ayrıca gerekli olması hâlinde ilgili tüm harici noktalarının uygun bir şekilde bilgi güvenliği ile ilgili değişen yasal ve teknik koşullar hakkında bilgilendirildiği bir yöntem (bkz. Ek A 1) OLUŞTURULMALIDIR ve ENTEGRE EDİLMELİDİR.

Yöntem aşağıda belirtilen hususları SAĞLAMAK ZORUNDADIR:

1. Güvenli kaynaklardan düzenli aralıklarla bilgi güvenliği ile ilgili güncel teknik ve yasal gelişmeler, özellikle de yeni potansiyel zarar kaynakları ve olası karşı tedbirler hakkında bilgiler toplanmalıdır.
2. Değişen tehlike durumlarını algılamak için bilgiler, bilgi güvenliği bağlamında anlam ve önem konusunda zaman kaybedilmeden değerlendirilmelidir.
3. İlgili sorumlular ilgili gelişmeler konusunda zaman kaybedilmeden bilgilendirilmelidir.

Sorumluların güncel bilgi seviyesinde kalmaları, ayrıca sektörel bilgi ve bilgilendirmelere erişmeleri için ilgi grupları ve güvenlik forumları ile temas ve bağlantılar ETKİN ŞEKİLDE YÜRÜTÜLMELİDİR.

8.2 Hassasiyet Oluşturmak, Temel ve İleri Eğitim

Aşağıda belirtilen hususları garanti eden bir yöntem (bkz. Ek A 1) GELİŞTİRİLMELİDİR ve ENTEGRE EDİLMELİDİR:

1. İlgili personel hedef grup odaklı bir şekilde potansiyel zarar kaynakları konusunda bilgilendirilir ve mevcut güvenlik tedbirlerinin uygulanması hakkında eğitilir.
2. BG yönetmeliği ve tüm ilgili BG yönergelerinin içerikleri aktarılır.
3. Bağlayıcı talimat ve kurallara uyulmadığında ortaya çıkan sonuçlar hakkında bilgi verilir.

Eğitim ve hassasiyetin oluşturulmasına yönelik tedbirler, personelin konuları anlayıp anlamadığını belirlemek için bir Bilgi Testi ile TAMAMLANMALIDIR.

9 Kritik IT (BT) Kaynaklarının Belirlenmesi

BGS, işletmenin kritik IT kaynaklarını belirlemek, yılda bir kere kritik IT kaynakları listesinin güncel olup olmadığını kontrol etmek ve gerekli ise onu uyarlamak ZORUNDADIR.

İşletme bu nedenle İş Sürekliliği Yöntemi (Business Continuity Management / BCM, bkz. Bölüm 17) çerçevesinde yılda bir kere BSI-Standart 100-4 veya DIN EN ISO 22301 gibi genel kabul gören standartlar temelinde bir İş Etki Analizi (Business Impact Analyse) veya BSI-Standart 100-2 temelinde bir Koruma İhtiyacı Analizi GERÇEKLEŞTİRMELİDİR.

Farklı bir hareket tarzı seçilirse, aşağıda belirtilen bölümlerin gereklerini karşılayan bir yöntem (bkz. Ek A 1) ENTEGRE EDİLMELİDİR.

9.1 Süreçler

İşletme, ana iş süreçlerini ve yüksek bir hasar ve/veya zara potansiyeline sahip olan süreçlerini tanımlamak ve belgelemek ZORUNDADIR.

Bu dokümantasyon, aşağıda belirtilen talepleri KARŞILAMAK ZORUNADIR:

1. Sürecin kısa bir açıklamasını içerir.
2. Sürecin neden ana bir iş süreci veya yüksek hasar ve/veya zara potansiyeline sahip bir süreç olduğunu açıklar.
3. Süreç için kimin yetkili olduğunun bilgisini içerir (süreç sorumlusu).
4. Sürecin tolore edilebilen azami devre dışı kalma süresi ile ilgili bilgiyi içerir (azami tolore edilebilen devre dışı kalma süresi – ATDDKS).

Süreç listesi ve bunlara ait dokümantasyon üst yönetim tarafından ONAYLANMALIDIR.

9.2 Bilgiler

İşletme, özel koruma tedbirleri gerektiren bilgileri belirlemek zorundadır.

Aşağıda belirtilen faktörlerin vahim hasarlara ve/veya zararlara neden olabildiği tüm bilgiler özellikle korunmalıdır:

1. Yetkisiz inceleme, bilgi edinme veya iletim ("Gizlilik" kriteri)
2. Değiştirilmesi ("Bütünlük" kriteri)
3. Geri dönülmez şekilde kaybedilmesi ("Uzun vadeli kullanılabilirlik" kriteri)
4. Kısa süreli hizmette olmaması durumu ("Anlık kullanılabilirlik" kriteri)

Kritik bilgileri belirlemek için ana iş süreçleri ve yüksek zarar ve/veya hasar oluşturma potansiyeline sahip süreçler (bkz. Bölüm 9.1) incelenmelidir ve bilgilerin hem türü hem kapsamı dikkate alınmalıdır.

9.3 IT (BT) Sistemleri, Mobil Veri Taşıyıcıları ve Bağlantılar

İşletme, kendine ait kritik IT (BT) sistemlerini, mobil veri taşıyıcılarını ve bağlantılarını berlirlemek ZORUNDADIR.

IT (BT) sistemleri, mobil veri taşıyıcıları ve bağlantılar, onlarla kritik bilgiler (bkz. Bölüm 9.2) işleniyor, depolanıyor veya aktarılıyor ise kritik olarak tanımlanmaktadır.

Her kritik IT (BT) sistemi için, her kritik mobil veri taşıyıcısı için ve her kritik bağlantı için ATDDKS (azami tolore edilebilen devre dışı kalma süresi) belirlenmelidir. ATDDKS, IT

sistemine, mobil veri taşıyıcısına veya bağlantıya bağlı olan tüm kritik süreçlerin en kısa ATDDKS kadar kısa veya bundan daha kısa olmak ZORUNDADIR (bkz. Bölüm 9.1).

Kritik IT (BT) sistemlerini, mobil veri taşıyıcıları ve bağlantıları tespit etmek için bir Top-Down yaklaşımı (süreç odaklı bakış), bir Bottom-Up yaklaşımı (sistem odaklı bakış) veya her ikisinden oluşan bir karışım UYGULANABİLİR. Top-Down yaklaşımda, kritik bilgilerin (bkz. Bölüm 9.2) nerede işlendiği, depolandığı ve nereden nereye aktarıldığı tespit edilmektedir. Buna karşın Bottom-Up yaklaşımında işletmeye ait IT (BT) sistemleri, mobil veri taşıyıcıları ve bağlantılar, kritik bilgileri işleyip işlemedikleri, depolayıp depolamadıkları ve aktarıp aktarmadıkları konusunda incelenmektedir. Her iki yaklaşımdan oluşan bir karışım, kritik IT (BT) sistemlerinin, veri taşıyıcılarınnı ve bağlantıların güvenilir bir şekilde belirlenmesi olanağı sunmaktadır.

Kritik IT (BT) sistemlerinin, mobil veri taşıyıcıların ve bağlantıların belirlenmesinden sonra, IT (BT) alt yapısının hangi bölümlerinin işletim için mutlaka gerekli olduğu TESPİT EDİLMELİDİR. IT (BT) alt yapısının bu bölümleri de kritiktir.

9.4 Özgün Yazılımlar

İşletme, kritik özgün yazılımlarını belirlemek ZORUNDADIR.

Kritik özgün yazılımlar, IT (BT) sistemlerinin (bkz. Bölüm 9.3) işletilmesi için mutlaka gerekli olan ve özgün olarak işletme için oluşturulmuş veya uyarlanmış yazılımlardır.

10 IT (BT) Sistemleri

Bir işletmeye ait bilgi işleme süreci, büyük ölçüde elektronik şekilde gerçekleşmektedir. Bu nedenle IT (BT) sistemlerinin düzenli bir şekilde yönetilmesi ve emniyete alınması gereklidir.

10.1 Envanter Listesi

İşletmeye ait tüm IT (BT) sistemlerinin kayıtlı olduğu bir envanter listesi mevcut OLMALIDIR.

Envanter listesi uygun yöntemlerle (bkz. Bölüm 10.2.1 ve 10.2.2) eksiksiz ve güncel durumda TUTULMALIDIR.

Bu liste içinde her IT (BT) sistemi için aşağıda belirtilen bilgiler kaydedilerek BELGELENMELİDİR:

1. Yanlış anlaşılmaya fırsat vermeyecek tanımlama özelliği
2. Hızlı bir lokalizasyona izin veren bilgiler
3. Kullanım amacı

Bununla birlikte kurulum ve konfigürasyon ile ilgili özel hususlar dokümantasyona DÂHİL EDİLMELİDİR.

10.2 Yaşam döngüsü

10.2.1 İşletime alım ve değiştirme

IT (BT) sistemlerinin devreye alınması ve değiştirilmesi için bir yöntem (bkz. Ek A 1) oluşturulmalı ve entegre edilmelidir. Bu yöntem aşağıda belirtilen hususları GARANTI ETMELIDIR:

1. IT (BT) sisteminin kritik olup olmadığı belirlenir (bkz. Bölüm 9.3).
2. IT (BT) sistemlerinin envanteri (bkz. Bölüm 10.1) ve ağlarin dokümantasyonu (bkz. Bölüm 11.1) güncellenir.
3. Temel koruma (bkz. Bölüm 10.3) uygulanır.
4. Devreye alınma süreci esnasında ön ayarlı kimlik doğrulama özellikleri (örn. standart şifreler) değiştirilir veya ilgili girişler devre dışı bırakılır.
5. Devreye alınma süreci esnasında iş adımları ilgili sorumlu tarafından yazılı bir şekilde teyit edilir.

10.2.2 Kullanımdan Kaldırım Ve Yeniden Kullanım

IT (BT) sistemlerinin devre dışı bırakılması ve yeniden kullanılması için bir yöntem oluşturulmalı (bkz. Ek A 1) ve entegre edilmelidir. Bu yöntem aşağıda belirtilen hususları GARANTI ETMELIDIR:

1. IT (BT) sistemlerinin envanteri (bkz. Bölüm 10.1) ve ağlarin dokümantasyonu (bkz. Bölüm 11.1) güncellenir.
2. IT (BT) sistemi, kayıtlı bilgiler konusunda incelenir.
3. Bilgilerin emniyete alınıp alınmayacağı ve arşivlenip arşivlenmeyeceği, ve bu işlemler gerçekleştirilecekse bunların nasıl yapılacağı konusu kontrol edilir.
4. IT (BT) sistemi üzerinde kayıtlı bilgilerin, sürekli kullanılabilir olmaları gerekiyorsa, arşivlenmiş olduğu kontrol edilir (bkz. Bölüm 9.2).
5. Tüm bilgiler yetkisiz erişimden, güvenli bir şekilde silinerek, üzerileri yazılarak, IT (BT) sistemi içinden uzaklaştırılarak veya IT (BT) sisteminin tamamının imha edilmesi ile korunur.
6. Tüm iş adımları ilgili sorumlu tarafından yazılı bir şekilde teyit edilir.

10.3 Temel Koruma

Aşağıda sunulan bölümlerdeki tedbirler, şayet ilgili bir işlevsellik mevcut ise, tüm IT (BT) sistemleri için OLUŞTURULMALI VE ENTEGRE EDİLMELİDİR.

Şayet tedbirler uygun bir işlevsellik mevcut olmasına rağmen uygulanmazsa, bu durum nedeniyle oluşan risk için karsi tedbirler, risk analizi ve risk yönetimi desteği (bkz Ek A 2) ile YÜRÜRLÜĞE KONULMALIDIR.

10.3.1 Güncellemeler

Sistem ve uygulama yazılımları için üretici tarafından hizmete sunulan güvenlik güncellemeleri entegre edilmiş bir yönteme (bkz. Ek A 1) uygun şekilde TEST EDİLMELİDİR, uygunlukları ONAYLANMALIDIR ve onaylandıktan sonra derhal KURULMALIDIR.

10.3.2 Ağ Trafiğinin Sınırlandırılması

IT (BT) sistemine giden ve ondan gelen ağ trafiği, aşağıdaki kriterlerden herhangi birini sağlıyor ise, işlevsellik için gerekli olan asgari ölçüyle SINIRLANDIRILMALIDIR.

1. Ağ üzerinde istismar edilebilen ve giderilemeyen (örn. güvenlik güncellemeleri kurulamıyor, şifreler değiştirilemiyor veya güvenli olmayan teknik yöntemler kullanılıyorsa) zayıf noktalar mevcut.
2. Özel tasarıma sahip bir IT (BT) sistemi söz konusu (örn. İnternet üzerinden erişilebilir olan veya kamuya açık mekânlara yerleştirilmiş olan IT (BT) sistemleri).

10.3.3 Raporlama

Her IT (BT) sistemi kullanıcıların giriş ve çıkışlarını, hataları ve bilgi güvenliği ile ilgili olayları raporlamak ZORUNDADIR.

Rapor verileri merkezi bir şekilde KAYDEDİLMELİDİR.

Rapor verileri, şayet silme ve saklama yükümlülükleri ile ilgili farklı yasal düzenlemeler mevcut değilse 6 ay SAKLANMALIDIR.

Tüm IT (BT) sistemleri, log kayıtlarının değerlendirilmesine olanak sağlamak için ortak bir saate SENKRONİZE EDİLMİŞ OLMALIDIR.

10.3.4 Harici Arabirimler Ve Sürücüler

İş süreçleri için gerekli olmayan harici arabirimler ve sürücüler, SÖKÜLMELİDİR, DEVRE DIŞI BIRAKILMALIDIR veya başka bir şekilde kullanıcılar için ERİŞİLEMEZ duruma getirilmelidir.

10.3.5 Zararlı Yazılımlar

Tüm IT (BT) sistemleri zararlı yazılımlara karşı korumaya SAHİP OLMALIDIR.

Her IT (BT) sistemi uygun yazılımlar yardımıyla her gün eksiksiz şekilde zararlı yazılımların varlığı konusunda DENETLENMELİDİR.

Ayrıca tüm IT (BT) sistemleri, erişilen tüm dosyaları zararlı yazılımlar konusunda denetleyen gerçek zamanlı korumaya SAHİP OLMALIDIR.

Gerçek zamanlı koruması olan IT (BT) sistemlerinde zararlı yazılımlar konusundaki eksiksiz denetim, haftalık bir ritme DÜŞÜRÜLEBİLİR.

Algılanan zararlı yazılımların çalıştırılması mutlaka ÖNLENMELİDİR.

Zararlı yazılımlara karşı koruma sağlayan yazılım, otomatik şekilde her gün üreticilerin en yeni arama metotları için arama yapmak ZORUNDADIR ve bu arama metotlarını KULLANMALIDIR.

10.3.6 Yabancı Medyaların Başlatılması

IT (BT) sistemlerinin sadece yetkili medyalar tarafından başlatılması SAĞLANMALIDIR.

Bu örn. BIOS şifreleri veya IT sistemi için yerleştirilen fiziksel bir koruma ile SAĞLANABİLİR.

10.3.7 Kimlik Doğrulama Süreci

IT (BT) sistemlerinin kamuya açık olmayan alanlarına erişim, kimlik doğrulama talep eden uygun giriş yöntemleri ile EMNİYETE ALINMALIDIR.

Giriş yöntemleri aşağıda belirtilen hususları sağlamak ZORUNDADIR:

1. Giriş bilgilerinin sistematik şekilde denenmesi zorlaştırılır.
2. Başarılı ve başarısız giriş denemeleri raporlara kaydedilir.
3. Etkileşimli oturumlar, kullanıcı ön ayarlı bir süre dâhilinde hiçbir giriş yapmazsa sonlandırılır veya kilitlenir.

4. Giriş bir sosyal ağ üzerinden gerçekleşiyorsa, o zaman giriş bilgileri için güvenilirlik ve bütünlük (örn. Uygun kimlik doğrulama protokolleri ile) sağlanır.

Giriş yöntemlerinin güvenli şekilde çalışması için, aşağıda belirtilen hususlar SAĞLANMALIDIR:

1. Girişler yapılandırılmış bir şekilde yönetilir (bkz. Bölüm 15).
2. Güvenilir kimlik doğrulama mekanizmaları kullanılır.
3. Basit kimlik doğrulama özellikleri (örn. tahmin edilmesi kolay şifreler) kullanılmaz.

10.3.8 Erişim Kısıtlamaları

Uygun erişim kısıtlamaları yardımı ile, kullanıcının yönetimsel işleri yapamaması GARANTİ EDİLMELİDİR.

Ayrıca uygun erişim kısıtlamaları ile aşağıda belirtilen talepler KARŞILANMALIDIR:

1. *Kullanıcılar sadece, görevlerini yerine getirmek için gerekli olan bilgilere erişebilir.*
2. *Kullanıcılar sadece, görevleri gereği bu gerekli ise bilgilere yazma yetkisi ile erişebilir.*

10.4 Mobil IT (BT) Sistemleri İçin Ek Tedbirler

Mobil IT (BT) sistemleri özellikle hırsızlık, yetkisiz erişimler veya güvenli olmayan ağlar gibi özel tehlikelere maruz oldukları için ek tedbirler alınması gerekmektedir.

Tüm mobil IT (BT) sistemleri için aşağıda belirtilen tedbirler, Bölüm 10.3 içinde açıklananlara ek olarak UYGULANMALIDIR.

10.4.1 BG Yönergesi

Bölüm 6 içindeki kurallara ek olarak mobil IT (BT) sistemlerinin kullanımı bir BG yönergesi içinde BELİRLENMELİDİR.

BG yönergesi aşağıda belirtilen hususları sağlamak ZORUNDADIR:

1. İşletmeye ait hangi bilgilerin mobil IT sistemleri ile toplanabildiği, işlenebildiği, kaydedilebildiği ve aktarılabildiği belirlenir.
2. Veri güvenliği için sorumluluk tanımlanır.
3. Kullanıcılar mobil IT (BT) sistemlere özel riskler (örn. kamuya açık yerlerde kullanım esnasında başkaları tarafından izlenme nedeniyle oluşan tehlikeler, kayıp ve hırsızlık nedeniyle oluşan tehlikeler) hakkında bilgilendirilir ve uygun karşı tedbirler almakla yükümlüdür.
4. Mobil IT (BT) sistemlerinin yetkisiz üçüncü kişilere verilmesi yasaklanır.
5. Mobil IT (BT) sistemleri üzerine, kullanıcı tarafından yazılım kurulmasına izin verilip verilmediği, ayrıca hangi yazılımların kurulabileceği hususları tanımlanır.
6. Sistem yöneticisinin mobil IT (BT) sisteminin yerini belirleyip belirleyemeyeceği ve bu işlemi hangi koşullar altında yapabileceği tanımlanır.
7. Sistem yöneticisinin mobil IT (BT) sistemi üzerindeki bilgileri uzaktan silme yetkisine sahip olup olmayacağı, ayrıca hangi koşullar altında silebileceği hususları tanımlanır.

10.4.2 Bilgilerin Korunması

Mobil IT (BT) sistemleri üzerinde kayıtlı olan işletmeye ait bilgiler, gizlilik ve bütünlük ihlaline karşı KORUNMALIDIR.

Gizliliğin korunması örn. veri taşıyıcıların şifrelenmesi ile sağlanabilir.

10.4.3 Kayıp

Kullanıcıların ve sistem yöneticilerinin mobil IT sistemi kaybolduğunda nasıl hareket edeceğini tanımlayan bir yöntem OLUŞTURULMALI VE ENTEGRE EDİLMELİDİR (bkz. Ek A 1).

Bu yöntem özellikle, kaybın ne şekilde ve kime bildirileceğini ve akabinde hangi işlemlerin gerçekleştirileceğini BELİRLEMELİDİR.

Yöntem, işletmeye ait cihaz üzerindeki girişlerin, kayıp bildiriminden sonra artık yetkisiz bir şekilde kullanılamayacağını GARANTİ ETMELİDİR (örn. ilgili kimlik doğrulama özellikleri derhal sıfırlanarak, çağrı yönlendirmeleri değiştirilerek veya sesli mesajlar silinerek).

Mobil IT (BT) sisteminin kaybolması, güvenlik ihlali olarak (bkz. 18) ELE ALINMALIDIR.

10.5 Kritik IT (BT) Sistemleri İçin EK Tedbirler

Aşağıda belirtilen tedbirler, Bölüm 10.3 içinde açıklananlara ek olarak tüm kritik IT (BT) sistemleri için UYGULANMALIDIR.

Şayet tedbirler uygulanmazsa, bu durum nedeniyle oluşan risk için karşi tedbirler risk analizi ve risk yönetimi desteği (bkz Ek A 2) ile YÜRÜRLÜĞE KONULMALIDIR.

10.5.1 Risk analizi Ve Risk Yönetimi

Kritik IT (BT) sistemleri için bir risk analizi ve risk yönetimi süreci UYGULANMALIDIR (bkz. Ek A 2).

10.5.2 Acil Durum İşletim Seviyesi

Her kritik IT (BT) sistemi için bir "acil durum işletim seviyesi" tanımlanmalıdır.

10.5.3 Dayanıklılık

Kritik IT (BT) sistemleri üzerinde geliştirmelerin veya testlerin gerçekleştirilmesi YASAKTIR.

Kritik IT (BT) sistemleri üzerindeki, görevlerin yerine getirilmesi için gerekli olmayan her türlü ağ hizmeti KALDIRILMALIDIR; KAPATILMALIDIR veya uygun filtre mekanizmaları ile ERİŞİLEMEZ duruma getirilmelidir.

Kritik IT (BT) sistemleri üzerindeki, görevlerin yerine getirilmesi için gerekli olmayan her türlü uygulama yazılımı KALDIRILMALIDIR.

Uygulama yazılımlarının kritik IT (BT) sistemleri üzerindeki tüm erişim yetkileri ve özgün hakları, asgari bir ölçüye INDIRILMELIDIR.

10.5.4 Harici Arabirimler Ve Sürücüler

İş süreçleri için gerekli olmayan harici arabirimler ve sürücüler, SÖKÜLMELİDİR, DEVRE DIŞI BIRAKILMALIDIR veya başka bir şekilde kullanıcılar için ERİŞİLEMEZ duruma getirilmelidir.

10.5.5 Değişikliklerin Yönetilmesi

Kritik IT (BT) sistemleri üzerinde gerçekleştirilecek olan değişiklikler, önce bir test ortamında TEST EDİLMİŞ VE ONAYLANMIŞ OLMALIDIR.

Değişiklik nedeniyle IT (BT) sisteminde hatalı fonksiyonların oluşması veya değişiklik nedeniyle IT sisteminin devre dışı kalması durumu için kritik IT (BT) sistemleri, onu ATDDKS (azami tolore edilebilen devre dışı kalma süresi) dâhilinde tekrar asıl (değişiklikten önceki duruma) geri getirilmesini garanti eden bir mekanizma ile DONATILMIŞ DURUMDA OLMALIDIR.

10.5.6 Dokümantasyon

Her kritik IT (BT) sistemi için bir dokümantasyon mevcut olmak ZORUNDADIR.

Dokümantasyon kullanılarak uzmanlık bilgisine sahip personel, aşağıda belirtilen hususları geriye dönük takip edebilmelidir:

1. IT (BT) sisteminin sorumlusunun kimliği
2. IT (BT) sistemine yönetimsel erişimin nasıl ve hangi giriş ve kimlik doğrulama özellikleri ile mümkün olduğu
3. Kurulum esnasında hangi temel tasarım kararlarının alındığı
4. Hangi değişikliklerin gerçekleştirilmiş olduğu
5. Değişikliklerin ne zaman yapıldığı
6. Değişikliklerin kim tarafından yapıldığı
7. Değişikliklerin neden yapıldığı

10.5.7 Veri Yedekleme

Tüm kritik IT (BT) sistemleri verilerin yedeklenmesine hizmet eden bir sürece (bkz. Bölüm 16) sahip olmak ZORUNDADIR.

10.5.8 Denetim

Kritik IT (BT) sistemlerinin standart işletimde bulunup bulunmadığı DENETLENMELİDİR.

Bu esnada, kritik bir IT (BT) sisteminin devre dışı olup olmadığının algılanması ve uygun karşı tedbirlerin tetiklenmesi GARANTİ EDİLMELİDİR.

Ayrıca kritik IT (BT) sistemlerinin kaynakları, akut duruma gelmeden kaynak yetersizliklerini algılamak için DENETLENMELİDİR.

10.5.9 Yedek Sistemler ve Yöntemler

Kritik bir IT (BT) sistemi ATDDKS (azami tolore edilebilen devre dışı kalma süresi) dâhilinde kurulamaz ise, işletme, bu IT (BT) sistemine bağlı olan kritik süreçleri devam ettirebileceği yedek bir sisteme veya yönteme SAHİP OLMAK ZORUNDADIR.

Yedek sistem veya yöntem, kritik IT (BT) sisteminin 'acil durum işletim seviyesini' (bkz. 10.5.2) GARANTİ ETMELİDİR.

10.5.10 Kritik Özgün Yazılımlar

İşletme sözleşme ve/veya organizasyonel düzenlemeler ile kritik özgün yazılımların (bkz. Bölüm 9.4) gelecekte de kullanılabilirliğini ve ihtiyaçlara uyarlanabileceğini SAĞLAMALIDIR.

11 Ağlar ve Bağlantılar

Ağlar ve bağlantılar bilgileri aktarırlar ve IT (BT) sistemlerini birbirine bağlamaktadırlar. Bu nedenle uygun şekilde emniyete alınmaları gereklidir.

11.1 Dokümantasyon

İşletmenin ağları hakkında uzmanlık bilgisine sahip personelin, aşağıda belirtilen hususları geriye dönük takip edebileceği şekilde dokümantasyon OLUŞTURULMALIDIR:

1. Aktif ağ bileşenleri
2. Birbirleri arasındaki bağlantılar
3. Harici ağlar ile bağlantılar
4. Görev
5. Fiziksel medyalar

11.2 Aktif Ağ Bileşenleri

Aktif ağ bileşenleri IT (BT) sistemleridir ve Bölüm 10 içinde açıklandığı şekilde ele alınmalıdırlar.

11.3 Ağ Geçitleri

Güvenli olmayan veya güvenliği yetersiz olan ağlara açılan ağ geçitleri için gerekli güvenlik tedbirleri risk analizi ve risk yönetimi kapsamı dâhilinde (bkz. Ek A 2) belirlenmelidir.

Güvenli olmayan veya güvenliği yetersiz olan ağlara ağ geçidini entegre eden ağ bileşenlerinin konfigürasyonu yılda bir kere KONTROL EDİLMELİDİR ve aşağıda belirtilen talepleri karşılamalıdır:

1. Güvenlik ile ilgili ayarlar için aşağıda belirtilen hususlar raporlara kaydedilmelidir:
   a. Bunlar kim tarafından entegre edildi
   b. Bunlar ne zaman entegre edildi
   c. Etkileri
   d. Neden gerekli oldukları
2. Hedeflenen trafik kısıtlamaları etkili bir şekilde uygulanmalıdır.

11.4 Temel Koruma

Aşağıda sunulan bölümlerdeki tedbirler, şayet ilgili bir işlevsellik mevcut ise, tüm ağlar için ENTEGRE EDİLMELİDİR.

Şayet tedbirler uygun bir işlevsellik mevcut olmasına rağmen uygulanmazsa, bu durum nedeniyle oluşan risk için karşı tedbirler risk analizi ve risk yönetimi desteği (bkz Ek A 2) ile YÜRÜRLÜĞE KONULMALIDIR.

11.4.1 Ağ Bağlantıları

Sürekli olarak kullanılmayan ağ bağlantıları, yetkisiz erişime karşı EMNİYETE ALINMALIDIR.

Bu örn. fiziksel bir erişim veya giriş kısıtlaması, ağların devre dışı bırakılması veya IT (BT) sistemlerinin kimlik doğrulaması üzerinden GERÇEKLEŞTİRİLEBİLİR.

11.4.2 Alt Bölümlere Ayırmak

İşletmeye ait ağların alt bölümlere ayrılması gerekliliği KONTROL EDİLMELİDİR ve verilen karar raporlara kaydedilmelidir.

Alt bölümlere ayırma işlemi mümkün olduğu kadar kapsamlı bir şekilde bağlantıların KISITLANMASINI, ayrıca bloke edilmiş bağlantıların RAPORLANMASI olanağını içermelidir.

11.4.3 Uzaktan Erişim

Güvenli olmayan veya güvenliği yetersiz olan ağlar üzerinden işletmeye ait kamuya açık olmayan verilere veya kamuya açık olmayan IT (BT) sistemlerine erişim EMNİYETE ALINMALIDIR.

Bu esnada aşağıda belirtilen talepler KARŞILANMALIDIR:

1. Aktarılan bilgilerin gizliliği, bütünlüğü ve doğruluğu korunmalıdır.
2. Erişim öyle düzenlenmelidir ki, sadece ilgili kullanıcının görevini yerine getirmesi için gerekli olan IT (BT) sistemleri erişilebilir durumda olmalıdır.

Ayrıca aşağıda belirtilen talepler KARŞILANMALIDIR:

1. Erişim bir Remote-Desktop bağlantısı üzerinden gerçekleştirilmelidir; bu bağlantı işletmeye ait verilerin erişimi gerçekleştiren IT (BT) sistemine kopyalanmasını önler.
2. Kullanıcı, özellikle de kapsamlı erişim yetkilerine sahip ise, bir çoklu kimlik doğrulama yöntemi ile doğrulanmalıdır, böylece yetkisiz erişim tehlikesi azaltılır.
3. Erişim öyle düzenlenmelidir ki, sadece kullanıcı değil, aynı zamanda erişimi gerçekleştiren IT (BT) sistemi de doğrulanır.

11.4.4 Ağların Birleştirilmesi

İşletmeye ait ağların güvenli olmayan veya güvenliği yetersiz olan ağlar üzerinden birleştirilmesi EMNİYETE ALINMALIDIR.

Bu esnada aktarılan bilgilerin gizliliği, bütünlüğü ve doğruluğu korunmalıdır.

11.5 Kritik Bağlantılar İçin Ek Tedbirler

Bölüm 11.4'e ek olarak kritik bağlantılar için bir risk analizi ve risk yönetimi süreci (bkz. Ek A 2) entegre edilmelidir.

12 Mobil Veri Taşıyıcıları

Mobil veri taşıyıcıları, korunmasız kullanım türleri nedeniyle özellikle tehlikeye açık durumdadır. Bu nedenle, bu duruma bağlı risklere uygun hareket edilmesi gereklidir.

12.1 BG Yönergesi

Bölüm 6 içindeki kurallara ek olarak mobil veri taşıyıcıların kullanımı bir BG yönergesi içinde BELİRLENMELİDİR.

BG yönergesi, aşağıda belirtilen talepleri ve özellikleri SAĞLAMAK ZORUNDADIR:

1. İşletmeye ait hangi bilgilerin mobil bir veri taşıyıcısına kaydedilebileceği belirlenir.
2. Kullanıcılar mobil veri taşıyıcılarının özel riskleri (örn. kamuya açık yerlerde kullanım esnasında başkaları tarafından izlenme nedeniyle oluşan tehlikeler, kayıp ve hırsızlık nedeniyle oluşan tehlikeler) hakkında bilgilendirilmelidirler ve kullanıcılar uygun karşı tedbirler almakla yükümlüdür.
3. Mobil veri taşıyıcıların yetkisiz üçüncü kişilere teslim edilmesi veya ödünç verilmesi yasaklanır.

12.2 Kritik Mobil Veri Taşıyıcıları İçin Ek Tedbirler

Aşağıda belirtilen tedbirler, Bölüm 12.1 içinde açıklananlara ek olarak tüm kritik mobil veri taşıyıcılar için UYGULANMALIDIR.

12.2.1 Risk analizi Ve Risk Yönetimi

Kritik mobil veri taşıyıcıları için bir risk analizi ve risk yönetimi süreci UYGULANMALIDIR (bkz. Ek 4).

12.2.2 Kayıtlı Bilgilerin Korunması

Kritik mobil veri taşıyıcıların üzerinde kayıtlı işletmeye ait bilgiler yetkisiz gözleme ve değişikliğe karşı KORUNMALIDIR.

Gizliliğin korunması örn. veri taşıyıcılarının şifrelenmesi ile sağlanabilir.

12.2.3 Kayıplar

Kullanıcıların ve sistem yöneticilerinin mobil bir veri taşıyıcısı kaybolduğunda nasıl hareket edeceğini tanımlayan bir yöntem ENTEGRE EDİLMELİDİR (bkz. Ek A 1).

13 Ortam

İşletme tüm IT (BT) sistemlerini ve veri hatlarını olumsuz çevre etkilerine karşı emniyete almak ZORUNDADIR.

Bu, örn. VdS 2007 gibi genel kabul gören standartlar temelinde GERÇEKLEŞTİRİLMELİDİR.

Farklı bir hareket tarzı seçilirse, aşağıda sunulan bölümlerde belirtilen talepleri karşılayan bir yöntem (bkz. Ek A 1) ENTEGRE EDİLMELİDİR.

13.1 Sunucular, Aktif Ağ Bileşenleri ve Ağ Dağıtım Noktaları

Sunucular, aktif ağ bileşenleri ve ağ dağıtım noktaları (örn. patch alanları) uygun tedbirlerle hasarlar ve yetkisiz fiziksel erişime karşı EMNİYETE ALINMALIDIR.

Bu örn. yapısal tedbirler (sunucu odası) veya kilitlenebilir dolaplar (sunucu ve ağ dolapları) ile GERÇEKLEŞTİRİLEBİLİR.

Sunucular, aktif ağ bileşenleri ve ağ dağıtım noktaları için aşağıda belirtilen gerekler BELİRLENMELİDİR ve bunların uygun yapısal, teknik ve organizasyonel tedbirlerle karşılanması SAĞLANMALIDIR:

1. *Ortam koşulları (örn. sıcaklık, havadaki nem oranı, toz veya duman)*
2. *Güç kaynağı*
3. *Temel hasarlara karşı koruma (ateş, su, yıldırım düşmesi ve aşırı yüksek gerilim)*
4. *Hırsızlığa karşı koruma*
5. *Yetkisiz fiziksel erişime karşı koruma*

13.2 Veri Hatları

Sabit şekilde döşenmiş olan veri hatları uygun yapısal tedbirlerle hasarlara karşı KORUNMALIDIR.

Bu örn. veri hatlarının kablo kanalları içine döşenmesi ile GERÇEKLEŞTİRİLEBİLİR.

Tüm veri hatları mutlaka genel geçerli standartlara - örn. DIN EN 50173/4 serisi - uygun şekilde DÖŞENMELİDİR.

13.3 Kritik IT (BT) Sistemleri İçin EK Tedbirler

Risk analizi ve risk yönetimi kapsamında (bkz. Bölüm 10.5.1) her kritik IT (BT) sistemi için aşağıda belirtilen tehditler ele alınmalıdır:

1. Uygunsuz ortam koşulları (örn. sıcaklık, havadaki nem oranı, toz veya duman)
2. Güvenilir olmayan güç kaynakları ve elektrik sistemleri
3. Temel hasarlar (ateş, su, yıldırım düşmesi ve aşırı yüksek gerilim)
4. Yetkisiz giriş, hırsızlık, sabotaj, vandalizm
5. Yetkisiz fiziksel erişim

14 IT (BT) Outsourcing ve Cloud Computing

IT (BT) kaynakları harici ortamlara aktarılıyorsa, işletmenin güvenliğe yönelik çıkarları dikkate alınmalıdır.

14.1 Hazırlık

IT (BT) kaynaklarının harici ortamlara aktarılmasına neden olan her türlü girişim, üst yönetim tarafından ONAYLANMALIDIR.

Her girişim için aşağıda belirtilen parametreler raporlara kaydedilmelidir:

1. Hangi IT (BT) kaynakları harici ortamlara aktarılacak

2. İşletmeye ait hangi kurallar, yasa ve sözleşmeler ile tanımlanan hangi kurallar, özellikle de harici ortama aktarılan IT (BT) kaynakları ile ilgili gizlilik, kullanılabilirlik ve bütünlük bağlamında tanımlanan hangi kurallar sağlanacak
3. Harici ortama aktarılan IT (BT) kaynakları kritik mi değil mi belirlenmelidir

IT (BT) kaynakları harici bir ortama aktarılacaksa, işletme aşağıda belirtilen adımlarla bu duruma HAZIRLAMALIDIR:

1. Harici bir ortama aktarılacak olan IT (BT) kaynaklarının yönetimi için uzmanlıklar (bilgi birikimi) oluşturulmalıdır.
2. IT (BT) alt yapısı harici ortama aktarılacak olan IT (BT) kaynakları ile uyum içinde çalışma konusunda hazırlanmalıdır.

14.2 Sözleşmenin Düzenlenmesi

IT (BT) kaynakları harici bir ortama aktarılacaksa, hizmet sağlayıcı ile bir sözleşme akdedilmelidir. Bu sözleşme Bölüm 14.1 içinde belirtilen talepleri içermelidir ve hizmet sunucusu bunları karşılayacağını TAAHHÜT ETMEK ZORUNDADIR.

Ayrıca sözleşme ihlalinden kaynaklanan tazminat taleplerinin hukuki yollardan tahsil edilebileceği, hizmet sağlayıcısı işletme ile aynı hukuki ortamda bulunmuyorsa da GARANTİ EDİLMELİDİR.

14.3 Kritik IT (BT) Kaynakları İçin Ek Tedbirler

Kritik IT (BT) kaynakları harici ortamlara (bkz. Bölüm 9) aktarılacaksa, Bölüm 14.1 içinde yer alan gizlilik, kullanılabilirlik ve bütünlük ile ilgili talepler bir risk analizi çerçevesinde BELİRLENMELİDİR ve sözleşme ile aşağıda belirtilen hususlar DÜZENLENMELİDİR:

1. Hizmetler
   a. Hizmet sağlayıcısı tarafından sağlanacak olan hizmetler tanımlanmalıdır, ayrıca bunların ölçülmesi ve denetlenmesi ile ilgili mutabakat sağlanmalıdır.
   b. Hizmetin sunulduğu konumlar (yerleşkeler) belirlenmelidir.
   c. Harici ortama aktarılan IT (BT) kaynaklarının korunması için hizmet sağlayıcısının alacağı güvenlik tedbirleri ile ilgili mutabakat sağlanmalıdır.
   d. İşletmenin IT (BT) altyapısı ve harici ortama aktarılmış olan IT (BT) kaynakları arasındaki arabirimler tanımlanmalıdır.
2. İletişim
   a. İşletmedeki ve hizmet sağlayıcısındaki iletişim kurulacak kişiler ismen belirlenmelidir.
   b. Bir gizlilik sözleşmesi imzalanmalıdır.
   c. Hizmet sağlayıcısının üçüncü kişilere verileri teslim edebileceği veya edemeyeceği, edebiliyorsa hangi koşullar altında veri teslim edebileceği konusunda bir mutabakat sağlanmalıdır.
   d. Harici ortama aktarılan IT (BT) kaynakları kapsamında hizmet sağlayıcısının güvenlik ile ilgili ihlallerdeki bilgilendirme yükümlülüğü konusunda bir mutabakat sağlanmalıdır.

3. Hizmette değişiklik yapılması ve sözleşmenin feshi
   a. Hizmet sağlayıcısının sözleşmenin feshi veya iflas durumundaki katkı sağlama yükümlülükleri, özellikle de işletmeye ait verilerin eksiksiz şekilde teslim edilmesi ve taşınma sürecinin hizmet sağlayıcısı tarafından etkin bir şekilde desteklenmesi sağlanmalıdır.
   b. Yukarıda belirtilen hususlarda birinde bir değişiklik söz konusu ise, bu husus yazılı bir şekilde raporlara kaydedilmelidir ve yazılı bir şekilde bildirilmelidir.
   c. Sözleşme ile belirlenmiş olan hizmetlerin yerine getirilmemesi durumunda oluşacak yükümlülükler de sözleşmeye kaydedilmelidir.

Ayrıca sözleşme ihlalinden kaynaklanan tazminat taleplerinin hukuki yollardan tahsil edilebileceği, hizmet sağlayıcısı işletme ile aynı hukuki ortamda bulunmuyorsa da GARANTİ EDİLMELİDİR.

15 Girişler Ve Erişim Yetkileri

Girişler ve erişim yetkileri, işletmeye ait kamuya açık olmayan IT (BT) sistemlerine ve verilerine erişime izin vermektedir. Bu nedenle her ikisi de uygun bir yapı içinde yönetilmelidir.

15.1 Yönetim

Girişlerin ve erişim yetkilerin oluşturulması ve değiştirilmesi, ayrıca kimlik doğrulama özelliklerinin sıfırlanması için aşağıda belirtilen hususları garanti eden yöntemler (bkz. Ek A 1) OLUŞTURULMALIDIR:

1. İlgili süreçler uygulamaya konulmadan önce ilgili birimden yazılı bir şekilde talep edilir ve bu merci tarafından kontrol edilir ve onaylanır.
2. Girişler ve erişim yetkileri sadece, bunlar ilgili kullanıcının görevlerini yerine getirmesi veya işletmenin dâhili süreçleri için gerekli ise onaylanır.
3. Bir kullanıcı yönetimsel girişlere veya erişim yetkilere sahip olacaksa, bu husus özel bir şekilde gerekçelendirilmelidir ve ilgili IT sorumlusu tarafından karara bağlanmalıdır.
4. Talebi sunan ve kullanıcı, zaman kaybedilmeden uygulama konusunda bilgilendirilmelidir; girişler kapatıldığında sadece talebi sunan bilgilendirilmelidir.
5. Bir giriş silinmeden önce, ona bağlı olan veriler aktarılır, silinir, emniyete alınır veya arşivlenir.
6. İlgili süreçler raporlara kaydedilmelidir.

15.2 Kritik IT (BT) Sistemleri Ve Veriler İçin Ek Tedbirler

Kritik IT (BT) sistemlerine ait tüm girişler (bkz. Bölüm 9.3), ayrıca kritik bilgilere sağlanan tüm erişim yetkileri (bkz. Bölüm 9.2) her yıl KAYDEDİLMELİDİR ve Bölüm 15.1 içinde açıklanan yönteme uygun şekilde oluşturulup oluşturulmadıkları ve gerekli olup olmadıkları konusunda kontrol edilmelidir.

Kurallara uygun oluşturulmayan girişler ve erişim yetkileri güvenlik ihlali olarak (bkz. Bölüm 18) ELE ALINMALIDIR.

16 Veri Yedekleme Ve Arşivleme

Veriler kullanılamaz hâle gelebilir veya kaybolabilir. Bu nedenle verilerin yedeklenmesi ile verilerin bütünlüğü ve kullanılabilirliği garanti edilmelidir.

Verilerin yedeklenmesi süreci, BSI-Standart 100-2 gibi genel kabul gören standartların temelinde, BSI'nin IT Temel Koruma Katalogları dikkate alınarak entegre edilmelidir.

Farklı bir hareket tarzı seçilirse, aşağıda belirtilen bölümlerin talepleri KARŞILANMALIDIR.

16.1 BG Yönergesi

Bölüm 6 içinde sunulan kural ve düzenlemelere ek olarak, işletmeye ait verilerin depolandığı yer bir BG Yönergesi dâhilinde BELİRLENMELİDİR.

İşletmenin verileri, verimli bir veri yedeklemeye olanak sağlamak için mümkün olduğunca MERKEZİ BİR ŞEKİLDE DEPOLANMALIDIR.

16.2 Arşivleme

İşletme, işletmenin dâhili taleplerini, yasal ve sözleşmelerden kaynaklanan talepleri karşılamak için hangi verilerin arşive kaydedileceğini KONTROL ETMELİDİR.

16.3 Yöntem

Verilerin yedeklenmesi, yeniden oluşturulması ve arşivlenmesi için aşağıda belirtilen hususları garanti eden yöntemler (bkz. Bölüm A 1) ENTEGRE EDİLMELİDİR:

1. Yedeklenen veriler aktarım, depolama ve taşıma durumunda değişikliklere, hasarlara, kaybolmaya ve yetkisiz gözleme karşı KORUNMALIDIR.
2. Yedeklenen veriler, yedeklenen IT (BT) sistemleri ile aynı yangın bölgesinde depolanmamalıdır.

Verilerin yedeklenmesi ve saklanması için oluşturulan münferit depolar, afet durumunda da yedeklenen verilerin hizmette olması için birbirinden uzak konumlarda muhafaza edilmelidir.

16.4 Geliştirme

BGS her yıl IT (BT) sistemlerinde, ayrıca işletmenin dâhili süreçlerinde, yasa ve sözleşmelerle tanımlanan çerçeve koşullarında meydana gelen değişikliklerin emniyete alma, tekrar oluşturma ve arşivleme yöntemlerinde bir uyarlamayı gerektirip gerektirmediğini KONTROL ETMEK ZORUNDADIR.

Gerekli uyarlamalar zaman kaybedilmeden ENTEGRE EDİLMELİDİR ve RAPORLARA KAYDEDİLMELİDİR.

16.5 Temel Koruma

Şayet uygun bir işlevsellik mevcut ise, aşağıda belirtilen bölümlerde sunulan tedbirler, depolama yerleri (bkz. Bölüm 16.1), sunucular, aktif ağ bileşenleri ve mobil IT sistemleri için ENTEGRE EDİLMELİDİR.

Tedbirler uygun bir işlevsellik mevcut olmasına rağmen uygulanmazsa, bu durum nedeniyle oluşan risk için karşı tedbirler risk analizi ve risk yönetimi desteği (bkz Ek A 2) ile YÜRÜRLÜĞE KONULMALIDIR.

16.5.1 Depolama Yerleri

Depolama yerleri öyle SAKLANMALIDIR ki, en son tekrar oluşturulabilir durumları 24 saatten eski olmamalıdır.

16.5.2 Sunucu

Sunucular öyle SAKLANMALIDIR ki, en son tekrar oluşturulabilir durumları (sistem yazılımları, konfigürasyonlar, uygulama yazılımları ve uygulama verileri) 24 saatten eski olmamalıdır.

16.5.3 Aktif Ağ Bileşenleri

Aktif ağ bileşenlerine ait sistem yazılımları ve konfigürasyonları, her değişiklikten sonra SAKLANMALIDIR.

16.5.4 Mobil IT (BT) Sistemleri

Verilerin yedeklenmesi için sistem yöneticileri tarafından teknik bir yöntem TANIMLANMALIDIR.

16.5.5 Testler

Yedekleme ve tekrar oluşturma yöntemleri TEST EDİLMELİDİR:

1. Yılda bir kere rastlantı prensibine uygun şekilde yedeklenen bir her IT (BT) sistemi, seçilmelidir ve bir test ortamında yeniden oluşturulmalıdır.
2. Yedekleme ve yeniden oluşturma yöntemindeki her değişiklikten sonra, etkilenen IT (BT) sistemlerinden biri yedeklenmeli ve bir test ortamında yeniden oluşturulmalıdır.

Testler, veri yedeklemeden sorumlu olan kişinin desteği olmadan GERÇEKLEŞTİRİLEBİLİR OLMALIDIR. Bunlar mevcut dokümantasyon kullanılarak farklı bir çalışan tarafından GERÇEKLEŞTİRİLMELİDİR.

Mevcut verilerin yedeklenmesi ve tekrar oluşturulması yöntemleri, testin sonuçları ve bulguları kullanılarak zaman geçirilmeden geliştirilmelidir.

Testin uygulanması ve sonuçları RAPORLARA KAYDEDİLMELİDİR.

16.6 Kritik IT (BT) Sistemleri İçin Ek Tedbirler

Her kritik IT (BT) sistemi, verilerin yedeklenmesi sürecine sahip OLMAK ZORUNDADIR; bu süreç Bölüm 16.5 içindeki taleplere ek olarak aşağıda belirtilen talepleri sağlamalıdır.

16.6.1 Risk Analizi

Risk analizi ve risk yönetimi (bkz. 10.5.1) kapsamında bir veri kaybının sonuçları ANALİZ EDİLMELİDİR ve bu esnada azami tolore edilebilen veri kaybı (ATEVK) ile ATDDKS (azami tolore edilebilen devre dışı kalma süresi) BELİRLENMELİDİR.

16.6.2 Yöntem

Verilerin yedeklenmesi ve tekrar oluşturulması için yöntemler aşağıda belirtilen hususları SAĞLAMALIDIR:

1. Kritik IT (BT) sistemleri eksiksiz şekilde saklanmaktadır (sistem yazılımları, konfigürasyonlar, uygulama yazılımları ve uygulama verileri).
2. ATEVK (azami tolore edilebilen veri kaybı) geçilmez.
3. Şayet yedek sistemler veya yöntemler hizmette değilse, verilerin ATDDKS (azami tolore edilebilen devre dışı kalma süresi) dâhilinde tekrar oluşturulması garanti edilmektedir (bkz. Bölüm 10.5.9).

16.6.3 Testler

Kritik IT (BT) sistemleri için yedekleme ve tekrar oluşturma yöntemleri yılda bir kere 16.5.5 uyarınca, kritik bir IT (BT) sistemi üzerinde TEST EDİLMELİDİR.

17 Arızalar ve Devre Dışı Kalma Durumları

Devre dışı kalma durumları için uygun bir reaksiyon, işletmeye normal operasyona hızlı bir şekilde dönme ve böylece hasarları asgari seviyede tutma olanağını sunmaktadır.

Bu amaçla işletme BSI-Standart 100-4 veya DIN EN ISO 22301 gibi genel kabul gören standartlara dayanan bir BCM (Business Continuity Management) entegre etmelidir.

Farklı bir hareket tarzı seçilirse, aşağıda belirtilen bölümlerin talepleri KARŞILANMALIDIR.

17.1 BG Yönergesi

Bölüm 6 içindeki kurallara ek olarak arızalar ve devre dışı kalma durumlarındaki hareket tarzı bir BG yönergesi içinde BELİRLENMELİDİR.

BG yönergesi aşağıda belirtilen hususları sağlamak ZORUNDADIR:

1. "Arıza" ve "Devre dışı kalma durumu" açık ve net bir şekilde tanımlanmaktadır.

   Bu kapsamda olası bir arızanın veya devre dışı kalma durumunun bildirilmesine hangi dikkati çekici unsurların sebep olacağının TANIMLANMASI ve listelenmesi GEREKLIDIR.
2. Her çalışan olası arızaları ve devre dışı kalma durumlarını bir sistem yöneticisine bildirmelidir.
3. Sistem yöneticileri, gerekli olması hâlinde ilgili süreç sorumlusu, IT (BT) sorumlusu ve BGS ile birlikte arızaları ve devre dışı kalma durumlarını öncelikle araştırmalıdır.
4. Hangi durumlarda üst yönetime arızalar ve devre dışı kalma durumları hakkında bilgi sunulacağı tanımlanmalıdır.
5. İşletme içinde ve dışarıya karşı, akut ve üstesinden gelinen arızalar ve devre dışı kalma durumları hakkında nasıl bir bilgilendirme stratejisi izleyeceği tanımlanmalıdır.

17.2 Reaksiyon

Arızalar veya devre dışı kalma durumları söz konusu olduğunda (bkz. Bölüm A 1) aşağıda belirtilen reaksiyonları burada sunulan sıralamayla SAĞLAYAN bir yöntem entegre edilmelidir:

1. Durumla ilgili bir genel bakış elde edilir.
2. İnsan sağlığını ve hayatını korumak için gerekli olan tüm tedbirler alınır.
3. Hasar derhal uygulamaya konulan tedbirlerle sınırlandırılır.
4. Hasar raporlara kaydedilir.
5. Kanıtlar emniyete alınır.
6. Hasar giderilir ve normal iş süreçlerine geri dönülür.
7. Nedenlerin belirlendiği ve somut iyileştirmelerin geliştirildiği müteakip bir çalışma gerçekleştirilir.

Küçük arızalarda veya devre dışı kalma durumlarında, yöntemi erken bir aşamada sonlandırmak MÜMKÜN OLMALIDIR.

17.3 Kritik IT (BT) Sistemleri İçin Ek Tedbirler

17.3.1 Tekrar Çalıştırma Planları

Her kritik IT (BT) sistemi için aşağıda belirtilen talepleri karşılayan bir tekrar çalıştırma planı oluşturulmalıdır:

1. Bu plan uzman personel için IT (BT) sistemini ATDDKS (azami tolore edilebilen devre dışı kalma süresi) dâhilinde acil durum işletim seviyesine ulaştırmak için gerekli olan tüm bilgileri, iş adımları ve bunların sırasını içermektedir.
2. Plan, gerekli kaynakları da içermektedir, örneğin: Personel ve ilgili iletişim bilgileri, donanım, yazılım, ağlar, hizmetler, şifreler.
3. Plan kolay anlaşılabilir ve düzenli bir yapıya sahiptir.
4. Plan acil bir durumda hızlı bir şekilde erişilebilir bir durumdadır.
5. Plan, ilgili IT (BT) sisteminden farklı bir yangın bölgesinde muhafaza edilmektedir.

17.3.2 Bağımlılıklar

Kritik IT (BT) sistemlerinin birbirleri arasındaki bağımlılıklar RAPORLARA KAYDEDİLMELİDİR.

Bu dokümantasyon aşağıda belirtilen talepleri KARŞILAMAK ZORUNADIR:

1. Bu dokümantasyon, kritik IT (BT) sistemlerinin hangi sırayla yeninden oluşturulacağını açık ve net bir şekilde tarif etmektedir.
2. Dokümantasyon kolay anlaşılabilir ve düzenli bir yapıya sahiptir.
3. Dokümantasyon acil bir durumda hızlı bir şekilde erişilebilir bir durumdadır.
4. Dokümantasyon, ilgili IT (BT) sisteminden farklı bir yangın bölgesinde muhafaza edilmektedir.

18 Güvenlik İhlalleri

Güvenlik ihlallerine uygun bir reaksiyon verilmesi işletmeye hasarları hızlı şekilde sınırlandırma ve giderme olanağını sunmaktadır. Bu nedenle işletme güvenlik ihlallerine uygun bir şekilde hazırlıklı olmalıdır.

18.1 BG Yönergesi

Bölüm 6 içindeki kurallara ek olarak güvenlik ihlalleri söz konusu olduğunda uygulanacak adımlar bir BG yönergesi içinde BELİRLENMELİDİR.

BG yönergesi aşağıda belirtilen hususları sağlamak ZORUNDADIR:

1. Güvenlik ihlali kavramı açık ve net şekilde tanımlanmalıdır.

   Bu esnada hangi dikkati çeken unsurların potansiyel bir güvenlik ihlalinin bildirilmesine neden olacağı listelenmelidir.
2. Her çalışan olası güvenlik ihlallerini BGS'ye bildirmelidir.
3. BGS'su güvenlik ihlallerini, gerekli olması hâlinde süreç sorumlusu ve sistem yöneticileri ile iş birliği yaparak öncelikle incelemelidir.
4. Hangi durumlarda üst yönetime güvenlik ihlalleri hakkında bilgi sunulacağı tanımlanmalıdır.
5. İşletmenin kendi içerisinde ve dışarıya karşı doğru, akut ve üstesinden gelinen güvenlik ihlalleri hakkında nasıl bir bilgilendirme yapacağı tanımlanmalıdır.

18.2 Fark etmek

İşletme, olası güvenlik ihlallerini fark etmek için uygun tedbirleri entegre ETMELİDİR; örn.

1. *Intrusion Detection Systeme (IDS)*
2. *Sağlama toplamına dayanan bütünlük kontrolü*
3. *Sensör sistemleri (Honeypots)*
4. *Hassas olan dosyalara erişimin denetlenmesi*
5. *Log mesajlarının kaydedilmesi ve değerlendirilmesi*

18.3 Reaksiyon

Güvenlik ihlalleri söz konusu olduğunda (bkz. Bölüm A 1) aşağıda belirtilen reaksiyonları burada sunulan sıralamayla SAĞLAYAN bir yöntem entegre edilmelidir:

1. Durumla ilgili bir genel bakış elde edilir.
2. İnsan sağlığını ve hayatını korumak için gerekli olan tüm tedbirler alınır.
3. Hasar derhal uygulamaya konulan tedbirlerle sınırlandırılır.
4. Hasar raporlara kaydedilir.
5. Kanıtlar emniyete alınır.
6. Hasar giderilir ve normal iş süreçlerine geri dönülür.
7. Nedenlerin belirlendiği ve somut iyileştirmelerin geliştirildiği müteakip bir çalışma gerçekleştirilir.

Küçük güvenlik ihlallerinde, yöntemi erken bir aşamada sonlandırmak MÜMKÜN OLMALIDIR.

Ek A

A.1 Yöntem

İşletme tüm bu yönergelerde talep edilen yöntemleri planlamalıdır, yönetmelidir ve sürekli şekilde iyileştirmelidir.

Bu, genel kabul gören bir kalite yönetim sistemi temelinde; örn.: DIN EN ISO 9001 çerçevesinde GERÇEKLEŞMELİDİR.

Farklı bir hareket tarzı seçilirse, aşağıda belirtilen talepler KARŞILANMALIDIR:

1. Tatbik süreci için kimlerin sorumlu olduğu tanımlanır.
2. Yöntemler, ilgili hedef grubu için erişilebilir ve anlaşılır bir şekilde tanımlanır, raporlara kaydedilir ve ilan edilir.
3. Yöntemler, yeterlilik, ve etkinlik bağlamında eksik veya kusurlar fark edildiğinde iyileştirilmelidir.
4. Uygulama, yeterlilik, ve etkinlik yılda bir kere yöntemlerin üçte birinde kontrol edilmelidir. Kontrol edilecek yöntemler rastlantı prensibine uygun şekilde seçilmelidir. Yıllık kontrol, kontrol edilen yöntemlerin yarısından fazlasının kusurlu olduğunun sonucunu veriyorsa, tüm yöntemler kontrol edilmelidir.

A.2 Risk analizi Ve Risk Yönetimi

İşletme bu yönerge ve talimatlarda talep edilen risk analizlerini gerçekleştirmek ZORUNDADIR ve fark edilen riskleri zaman kaybetmeden uygun şekilde ele almalıdır.

Bu süreç, genel kabul gören BSI-Standart 100-3, ISO/IEC 27005 veya ISO 31000 gibi standartlara dayanan bir risk yönetimi çerçevesinde OLMALIDIR.

Farklı bir hareket tarzı seçilirse, aşağıda belirtilen bölümlerin taleplerini karşılayan bir yöntem (bkz. Ek A 1) ENTEGRE EDİLMELİDİR.

A.2.1 Risk Analizi

Bir risk analizi aşağıda belirtilen talepleri karşılamak ZORUNDADIR:

1. Dokümantasyon, risklerin berlirlenmesi ve değerlendirilmesi için yöntemi ve iş adımlarını içerir.
2. Yöntem ve iş adımları, tehditlerin ve zayıf noktaların güvenli bir şekilde fark edilmesini garanti eder.
3. Risklerin değerlendirilmesi işletme için potansiyel hasarların ve bunların ortaya çıkma olasılıklarına dayanarak gerçekleştirilir.
4. Risk analizinin sonucu, risklerin ele alınmasında bir öncelik sırasının oluşturulmasına olanak sağlar.

A.2.2 Risklerin Ele Alınması

Tanımlanmış riskler zaman kaybedilmeden ve öncelikle ELE ALINMALIDIR, bunun için risklerin önlenmesi, azaltılması veya aktarılması için uygun tedbirler (örn. bir sigorta sözleşmesinin akdedilmesi ile) tanımlanmalıdır, raporlara kaydedilmelidir ve uygulanmalıdır.

Uygulama süreci KONTROL ve ETKİNLİĞİ TEST EDİLMELİDİR.

Riskler uygun bir şekilde ele alınamaz ise, bunlar üst yönetim tarafından KABUL EDİLMELİDİR ve bu husus raporlara kaydedilmelidir.

A.2.3 Tekrarlanma ve Uyarlanma

Risk analizleri yılda bir kere güncellik konusunda KONTROL EDİLMELİ ve ihtiyaç olması hâlinde TEKRARLANMALIDIR.

Risk analizleri ayrıca aşağıda belirtilen koşullardan biri ortaya çıkarsa zaman kaybedilmeden geliştirilmelidir:

1. Risk analizinin konusu önemli ölçüde değişmiştir (örn. donanım, yazılım veya bir IT sisteminin konfigürasyonu değiştirildi).
2. Risk analizinin konusunun kullanım amacı önemli ölçüde değişmiştir.
3. Potansiyel zarar kaynakları (tehlike oluşması durumu) artmıştır (örn. yeni tehlikeler algılanmış veya mevcut bir tehlike önemli ölçüde artmış ise).