



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

AĞ VE SİSTEM GÜVENLİĞİ YÖNETİM PROSEDÜRÜ

Doküman No	BGYS-PR14
Yayın Tarihi	06.07.2015
Revizyon Tarihi	13.03.2023
Revizyon No	02
Sayfa No	1 / 21

1.AMAÇ

Bu prosedürün amacı, Birimimiz bünyesinde bulunan ağ ve sistem mimarisi ve ağ altyapısı ile sistemlerin güvenli olarak çalışmasını sağlayacak esasları belirlemektedir.

2. KAPSAM

Ağ bağlantılı hizmetler, Birim personeli ve genelin kullanımına sunulan ağ erişimi hizmetini kapsamaktadır. Sistem hizmetleri; sistem kaynaklarını izleme ve tahsis etme, yedekleme yapma, kullanıcı hesaplarını yönetme vb. hizmetleri kapsamaktadır.

3.SORUMLULUKLAR

Bu prosedürden BGYS Yöneticisi sorumludur.

4. TANIMLAR VE KISALTMALAR

Kurum	: Gençlik ve Spor Bakanlığı Bilgi İşlem Dairesi Başkanlığı
Birim	: Ağ Yönetim Şubesi
BGYS	: Bilgi Güvenliği Yönetim Sistemi
Kullanıcı	: Gençlik ve Spor Bakanlığı çalışanları
USOM	: Ulusal Siber Olaylara Müdahale Merkezi
Kurumsal SOME	: Kurumsal Siber Olaylara Müdahale Ekibi
Sektörel SOME	: Sektörel Siber Olaylara Müdahale Ekibi
NAC	: Ağ Erişim Kontrolü
DHCP Sunucusu	: (Dinamik Ana Bilgisayar Yapılandırma Protokolü)IP adreslerinin bir ağ içerisindeki dağıtımını için otomatik ve merkezi bir yönetim sağlar.
LAN/VLAN	: Yerel Alan Ağı / Sanal Yerel Alan Ağı VLAN teknolojisi kullanılarak, LAN üzerindeki ağ kullanıcıları ve kaynaklar mantıksal olarak gruplandırılır ve portlara atanır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı

Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

**AĞ VE SİSTEM GÜVENLİĞİ YÖNETİM
PROSEDÜRÜ**

Doküman No	BGYS-PR14
Yayın Tarihi	06.07.2015
Revizyon Tarihi	13.03.2023
Revizyon No	02
Sayfa No	2 / 21

Dos/DDoS	: Dos (Servis Hizmet Reddi) saldırısı bir hedefe yönelik gerçekleştirilen, sistemin hizmet vermesini, kullanıcıların sisteme erişmesini engelleyen bir saldırı türüdür. DDos (Dağıtılmış Hizmet Reddi) ise saldırının bir kaynaktan değil de fazla sayıda farklı kaynaktan başlatılmasıyla gerçekleşir.
URL	:Tarayıcıda bir web sitesinin görüntülediği kısım
Sıfıncı Gün Atak Tespit ve Engelleme Sistemleri	Kötü niyetli ağ hareket ve bağlantılarının tespiti için kullanılan sistem
Antivirüs/Antispam Sunucuları	: Kurulu olduğu ağ üzerinde, o ağa bağlı olan uçlarda otomatik olarak son çıkmış olan virüslere ve ajanlara karşı savunma sistemi oluşturan sistem
Güvenlik Duvarı Cihazları	: Ağ trafiğini kontrol ederek istenmeyen erişimleri engellemeye yarayan yazılım veya donanım
Yük Dengeleme Cihazları	: Sunucular üzerindeki trafiği azaltıp dengeli olarak dağıtarak sunucuların ve üzerlerindeki servislerin güvenliğine katkı sağlayan teknoloji
İçerik Filtreleme Cihazları	: Web, eposta ve dosya transferleri trafiğini, güvenliğini yöneten sistem
IPS Cihazları	: Bir siber saldırı önleme sistemidir, sürekli olarak ağ üzerindeki trafiği takip eder ve kontrol eder.
Proxy (Vekil Sunucu) Cihazları	: İnternete erişim sırasında kullanılan bir ara sunucudur. Proxy, internet üzerindeki bir bilgisayar ile internete bağlı diğer bilgisayarlar arasındaki iletişimi sağlayan yardımcı bir geçiş yolu sistemidir.
Kablosuz Ağ Yönetim Cihazları	: Kablosuz bağlantılarınızı yönetmenize yardımcı olan cihazlar
Web Uygulama Güvenlik Duvarı	: Web uygulamalarının robotlar, enjeksiyon ve uygulama katmanı hizmet reddi (DoS) dahil olmak üzere kötü amaçlı saldırılara ve istenmeyen internet

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

AĞ VE SİSTEM GÜVENLİĞİ YÖNETİM PROSEDÜRÜ

Doküman No	BGYS-PR14
Yayın Tarihi	06.07.2015
Revizyon Tarihi	13.03.2023
Revizyon No	02
Sayfa No	3 / 21

	trafiğine karşı korunmasına yardımcı olur.
SSL Description Cihazları	: SSL Görünürlüğü olarak da adlandırılan SSL Şifre Çözme, trafiğin büyük ölçekte şifresini çözme ve onu, uygulamalara gelen ve kullanıcılardan internete giden tehditleri tanımlayan çeşitli inceleme araçlarına yönlendirme işlemidir.
Bant Genişliği Yönetim Cihazı	: Bant genişliği, internet ağı veya bir bilgisayar ağı üzerinde aktarılabilen maksimum veri miktarı olarak tanımlanmaktadır. Bant Genişliği Yönetim Cihazı ağlardaki verinin iletilme kapasitesini belirler.
SSL-VPN	: İstemci ve sunucu arasında internet üzerinden güvenli bir bağlantı sağlamak için taşıma katmanında kullanılan bir ağ protokolüdür. SSL VPN'ler, uzak kullanıcılara web tarayıcısı aracılığıyla uygulanır ve özel yazılım yüklenmesi gerektirmez.

5.UYGULAMA

5.1. Ağ ve Sistem Erişimi

Ağ Yönetim Şubesi personeli, diğer kullanıcıların yetkilendirmesini ve erişim kurallarının uygulanmasını sağlar. Sistem Yönetimi ve Donanım Şubesi, sistem kaynaklarını izleme ve tahsis etme, yedekleme yapma, kullanıcı hesaplarını yönetme vb. hizmetlerin uygulanmasını sağlar.

Birimimiz ağ ve sistem yapısı içerisindeki noktalara erişim talepleri e-posta/resmi yazı ile ağ yöneticisine iletilmelidir.

5.2. Ağ ve Sistem Bağlantı Kontrolü

- Sisteme dışardan bağlanmak ve yönetim konsollarına bağlanmak izin verilen güvenli bağlantılar dışında kesinlikle yasak olmalıdır. Bakım, ayar veya sorun gidermek için, ağ yöneticilerinin sunucuların bulunduğu odaya güvenlik kontrollerini geçerek ulaşması

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	AĞ VE SİSTEM GÜVENLİĞİ YÖNETİM PROSEDÜRÜ	Doküman No	BGYS-PR14
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	13.03.2023
		Revizyon No	02
		Sayfa No	4 / 21

gerekmektedir. Bunun yanında ağ ve sistem yöneticilerin acil durumlarda erişebilmesi için güvenli uzak bağlantı platformu ile yetkili personellerin gerekli yerlere erişimleri kontrol edilmelidir.

- Sistem yöneticileri sunucular genelinde en geniş yetkiye sahip personel olmalıdır. Sunucularda ve diğer tüm sistemlerde bakım yapmaları gerektiğinden geniş yetkilere sahip olmalıdırlar.
- Tüm kullanıcılar, kendi kişisel kullanımları için, benzersiz bir kimliğe (kullanıcı kimliği) sahip olmalıdır. Kullanıcı yetkilerinin oluşturulması, silinmesi ve belirli periyotlarda erişim haklarının gözden geçirilmesi gerekir. Bir kullanıcının öne sürdüğü kimliğini ispatlamak için uygun bir kimlik doğrulama tekniği kullanılmalıdır. Sadece yetki verilen kişiler güvenli bir bağlantı sağlayabilmelidir.

5.3. Ağ ve Sistem Hizmetlerinin Güvenliği

- Ağ hizmetlerinin güvenliği Veri Merkezi içindeki Güvenlik Duvarları cihazları, Sıfırıncı Gün Atak Tespit ve Engelleme Sistemleri, Antivirüs/Antispam Sunucuları, Yük Dengeleme Cihazları, İçerik Filtreleme Cihazları, IPS Cihazları, Proxy (Vekil Sunucu) Cihazları, Kablosuz Ağ Yönetim Cihazları, Web Uygulama Güvenlik Duvarı, SSL Decryption Cihazları, Bant Genişliği Yönetim Cihazı tarafından sağlanmaktadır. Ağ ve sistem cihazlarının bulunduğu Veri Merkezi parmak izi okuma ile giriş yapılabilen, kamera ve ortam izleme cihazları ile izlenebilen, alarm ve yangın söndürme sistemlerine sahip olan bir ortam olmalıdır. Katlarda bulunan ağ cihazları ise dış ortamdan kabinler sayesinde güvenli hale getirilmelidir ve bu kabinlere erişim sadece Ağ Yönetimi ve Sistem Yönetimi ve Donanım Şubesi personeli, ilgili teknik personel tarafından sağlanmalıdır. İşletim sistemlerine erişim güvenli bir oturum açma prosedürü ile kontrol edilmelidir.
- Sistem hizmetlerinin güvenliği; Sanallaştırma Sunucusu (Vcenter-ESXI-Hostlar), DC Sunucusu (Fiziksel), Yedekleme Cihazları, Data Domain, Storage Disk Üniteleri, Teyp Kütüphanesi, Kullanıcı işletim sistemleri, Kullanıcı Office Uygulamaları, Sunucu İşletim Sistemleri, Active Directory-Domain Servisleri, Kurumsal E-posta Servisleri, DHCP Sunucu

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

AĞ VE SİSTEM GÜVENLİĞİ YÖNETİM PROSEDÜRÜ

Doküman No	BGYS-PR14
Yayın Tarihi	06.07.2015
Revizyon Tarihi	13.03.2023
Revizyon No	02
Sayfa No	5 / 21

Servisleri, DNS Sunucu Servisleri, Dosya Sunucu Servisleri, FTP Sunucu Servisleri, GSB Drive Sunucu Servisleri, Yazdırma Sunucusu Servisleri, SCCM Merkezi Sistem Yönetimi Servisleri, KMS Kurumsal Lisans Yönetim Servisleri, WSUS Update Yönetim Servisleri, Vcenter Veri Merkezi Yönetim Servisleri, ESXI Sanallaştırma Hizmetlerinin Yönetim Servisleri, Yedekleme ve İş Sürekliliği Servisleri ile sağlanmaktadır.

6. DONANIM VARLIKLARININ ENVANTER YÖNETİMİ

- Sadece onaylı donanımların kurum ağına bağlanabilmesi için, 802.1x standardı veya NAC(Ağ Erişim Kontrolü) çözümleri kullanılarak kurum ağına bağlanan cihazlara kimlik denetimi yapılmalıdır.
- Veri saklama, işleme ve iletme yeteneği olan tüm donanımların güncel bir envanteri tutulmalı, yalnızca yetkilendirilmiş personelin varlık envanterine erişimi mümkün kılınmalıdır.
- Donanım envanteri en az; her bir donanımın ağ adresini, donanım adresini, makine adını, seri numarasını, markasını, modelini destek alınan tedarikçi sözleşme bilgilerini (bakım süresi, kapsamı vb.), donanımın sorumlusunu, sorumlu kişinin birimini ve donanımın kurum tarafından onaylı olup olmadığı bilgisini içermelidir. Donanım envanter içeriğinde yapılan değişiklikler kayıt altına alınmalıdır.
- Kurum ağına bağlı cihazlar tanımlanmalı, donanım varlık envanterindeki değişiklikler takip edilmelidir. Kurumun donanım envanterini güncel tutmak için tüm DHCP sunucularında ya da IP adres yönetim araçlarında kayıt mekanizmasının kullanımı sağlanmalıdır.
- Kullanım ömrünü tamamlayan cihazların veri depolama üniteleri (HDD, SSD, USB, disk, harici bellek vb.) güvenli bir şekilde imha edilmelidir. Kurum içinde tekrar kullanılması durumunda ise veri kurtarmaya imkân sağlamayacak şekilde güvenli silme işlemine tabi tutulduktan sonra kullanıma alınmalıdır.

7. YAZILIM VARLIKLARININ ENVANTER YÖNETİMİ

- Kurumda kullanılan tüm yazılımların (işletim sistemleri, donanım yazılımları, üçüncü parti yazılımlar, uygulama yazılımları vb.) güncel bir listesi tutulmalı ve listeye yalnızca

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

AĞ VE SİSTEM GÜVENLİĞİ YÖNETİM PROSEDÜRÜ

Doküman No	BGYS-PR14
Yayın Tarihi	06.07.2015
Revizyon Tarihi	13.03.2023
Revizyon No	02
Sayfa No	6 / 21

yetkilendirilmiş personelin erişimi mümkün kılınmalıdır.

- Yazılım envanter yönetim araçlarında, kurum tarafından yetkilendirilen işletim sistemleri dâhil olmak üzere en az; yazılımların adı, sürümü, yayımcısı, destek alınan tedarikçi sözleşme bilgileri (bakım süresi, kapsamı vb.), lisans bilgileri ve edinim tarihi bilgileri, yazılımın yüklendiği donanımlar kayıt altına alınmalı ve izlenebilir olmalıdır. Yazılım envanter içeriğinde yapılan değişiklikler kayıt altına alınmalıdır.
- Kurumun onaylı yazılım envanterine yalnızca üreticisi tarafından desteklenen yazılımlar dâhil edilmelidir. Yazılım envanterinde kayıtlı olan yazılımlar için güncelleme desteği devamlılığı sağlanmalıdır. Üreticisi tarafından sunulan destek hizmeti sona ermiş ancak iş gereksinimleri sebebi ile kullanılması gereken yazılımlar, yazılım envanterinde “üretici tarafından desteklenmeyen” olarak etiketlenmelidir.
- Kurum sistemlerindeki tüm yazılımlar için envanter yönetim araçları kullanılmalıdır. Söz konusu envanter yönetim araçları, yazılımların mevcut durumları ile ilgili raporlama yeteneğine sahip olmalıdır.

8. TEHTİD VE ZAFİYET YÖNETİMİ

- Zararlı yazılımların kuruma ait ve/veya kurum tarafından yönetilen kullanıcı uç nokta cihazları ve altyapı bileşenleri üzerinde çalışması, kaydedilmesi ve aktarılması engellenmelidir. Personelin beyaz listede bulunan uygulama kategorileri haricinde uygulama kurması engellenmelidir.
- Tüm sistemlerdeki yazılımların, mevcut iş gereksinimlerini karşılayacak ve yazılım üreticisi tarafından sağlanan en kararlı ve güncel güvenlik sürümleri ile çalıştırılmakta olduğu otomatik yazılım güncelleme araçları kullanılarak kontrol edilmelidir. Otomatik yazılım güncelleme araçlarının kullanılamadığı durumlarda uzman personel tarafından manuel olarak gerekli kontroller periyodik olarak yapılmalıdır.
- Son kullanıcıların, güvenlik sıkılaştırmaları kapsamında kurum tarafından uygulanması gerekli görülen konfigürasyonlara müdahale etmemesi ve beyaz listede bulunan

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

AĞ VE SİSTEM GÜVENLİĞİ YÖNETİM PROSEDÜRÜ

Doküman No	BGYS-PR14
Yayın Tarihi	06.07.2015
Revizyon Tarihi	13.03.2023
Revizyon No	02
Sayfa No	7 / 21

programlar haricinde program kurmalarının engellenmesi için son kullanıcı hesaplarının yerel yönetici yetkileri kaldırılmalıdır.

- Zafiyet içerdiği tespit edilen uygulamalar veya sunucular karantina networküne alınarak güncellenmesi yapılmalıdır. Zafiyet giderilmiyorsa uygulama kullanımından vazgeçilmelidir.
- Tespit edilen güvenlik açıklarının giderilmesi için hazırlanan rapora yönelik önceliklendirme risk analizi tabanlı yapılmalıdır.
- Kurumsal uygulamalar (web, DNS, e-posta, FTP vb. ile diğer uygulamalar) ve kurum ağındaki bileşenler, işletim sistemi ve paket yazılımlar kullanıma alınmadan önce bilgi güvenliği gereksinimleri dikkate alınarak gerekli güvenlik sıkılaştırmaları yapılmalıdır.
- Ağ bileşenlerinin güvenlik güncellemeleri başta olmak üzere işletim sistemlerine yönelik güncellemelerin ve yamaların üreticisi tarafından bildirilen en kararlı, güncel ve güvenilir sürüm dikkate alınarak yapıldığı, otomatik yazılım güncelleme araçları ile kontrol edilmelidir.
- Kurumdaki sistemler düzenli olarak zafiyet taramalarından geçirilmelidir. Güvenlik taramaları için oluşturulan hesaplar taramalar dışında başka faaliyetler için kullanılmamalıdır. Bu hesapların yetkileri sadece belirli IP adreslerinden gerekli makinelerle bağlanabilecek şekilde kısıtlanmalıdır. Bu hesaplar düzenli olarak kontrol edilmelidir. Geçmişte tespit edilen zafiyetlerin giderilip giderilmediği sonraki taramalarda kontrol edilmelidir. Zafiyet tarama raporları muhafaza edilmelidir.
- Kurum sistemlerinin tümünü kapsayacak şekilde port, servis ve protokol taramaları gerçekleştirilmeli, açık ve kullanımına ihtiyaç olmayan portlar tespit edilmeli, kullanılmayanlar kapatılmalıdır.

9. E-POSTA SUNUCUSU VE İSTEMCİ GÜVENLİĞİ

- E-posta gönderiminde kullanıcı adı ve parola kullanılarak kimlik doğrulaması yapılmalıdır. Tekrar yayınlama (relay) işlemine, belirlenen IP adresleri dışında izin verilmemeli ve e-

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

AĞ VE SİSTEM GÜVENLİĞİ YÖNETİM PROSEDÜRÜ

Doküman No	BGYS-PR14
Yayın Tarihi	06.07.2015
Revizyon Tarihi	13.03.2023
Revizyon No	02
Sayfa No	8 / 21

posta hizmet protokollerinden kullanılmayanlar kapatılmalıdır.

- Kurum tarafından onaylanmış, üretici tarafından desteği devam eden kararlı ve güncel sürüme sahip internet tarayıcıları ile e-posta istemcileri kullanılmalıdır. E-posta içeriğindeki zararlı bağlantılara erişim engellenmelidir.
- Spam e-postaları engellemek üzere DNS tabanlı filtreleme ve kara liste yöntemleri uygulanmalıdır. E-posta bombardımanı ve bağlantı temelli servis dışı bırakma saldırılarına karşı SMTP sunucusunda bağlantı sayısı sınırlama vb. yöntemler ile koruma sağlanmalıdır.
- Gelen/giden tüm e-posta hesaplarına ait içerikler, istenmeyen e-postalar ve e-posta ile yayılabilecek zararlı yazılımlara karşı güvenliği sağlamak amacıyla SMTP Gateway vb. sistemler kullanılarak kontrol edilmelidir.
- Sahte ya da bütünlüğü bozulmuş e-postaların geçerli etki alanlarına sızma ihtimalini azaltmak için SPF, DKIM vb. teknoloji ve standartlar kullanılmalıdır.
- Kurum politikaları ile belirlenmiş olan risk içeren izinsiz ve/veya çalıştırılabilir dosya türleri içeren e-posta veya e-posta ekleri engellenmelidir.
- E-posta sunucuları, varsayılan ayarlarıyla kullanılmamalı ve kullanıma alınmadan önce tüm sunucuların güvenlik sıkılaştırmaları yapılmalıdır. İstemci ve e-posta sunucuları arasındaki iletişimde bilinen zafiyet içermeyen güvenilir SSL/TLS sürümleri ile birlikte güvenli e-posta iletişim protokolleri (SMTPs, POP3s, IMAPs, HTTPs vb.) kullanılmalıdır.
- E-posta sunucuları internetten gelebilecek her türlü saldırıları önlemek üzere katmanlı güvenlik tasarımı prensiplerine göre yapılandırılmalıdır.
- Sadece kurum tarafından onaylı internet tarayıcısı ve e-posta istemcisi eklentileri kullanılmalıdır. E-posta istemcilerinde sadece kurum tarafından izin verilen betik kodları çalıştırılmalıdır.
- Kurum politikalarına göre gizlilik dereceli bilgi/veri içeren e-posta alışverişleri şifreli ve imzalı olarak yapılmalıdır. E-posta alışverişleri şifreli ve imzalı olarak yapıldığı durumda kullanılan sertifikalar kuruma özel olarak üretilmelidir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

AĞ VE SİSTEM GÜVENLİĞİ YÖNETİM PROSEDÜRÜ

Doküman No	BGYS-PR14
Yayın Tarihi	06.07.2015
Revizyon Tarihi	13.03.2023
Revizyon No	02
Sayfa No	9 / 21

10. ZARARLI YAZILIMLARDAN KORUNMA

- İstemci ve sunucu sistemlerinin tamamında zararlı yazılımdan korunma uygulamaları kullanılmalı ve zararlı yazılımdan korunma uygulamalarında en güncel yama dosyalarının bulunması ve imza veri tabanının güncel olması sağlanmalıdır.
- Kurumdaki tüm bilgisayarlar, taşınabilir diskleri otomatik olarak zararlı yazılım taramasından geçirecek şekilde yapılandırılmalıdır.
- Kurumdaki tüm bilgisayarlar, taşınabilir ortamlarda otomatik kod çalıştırılmasına izin vermeyecek şekilde yapılandırılmalıdır.
- Zararlı yazılımlardan korunma uygulaması üretici veya ilgili kurum tarafından önerilen şekilde yapılandırılmalı ve güncel tutulmalıdır.
- Antivirüs programı zararlı bir yazılım tespit ettiğinde merkez sunucuya iletmelidir. Merkez sunucunun düzenli olarak yedeği alınmalıdır. Merkez sunucu, logu kendi içerisinde tutmalıdır.

11. AĞ GÜVENLİĞİ

- Kurum ağlarına ait topolojiler güvenli bir şekilde tutulmalı ve güncelliği kontrol edilmelidir.
- Ağ cihazları endüstri standartları, en iyi uygulamalar ve üretici tavsiyelerine uygun olarak yapılandırılmalıdır. Varsayılan parola ve kullanıcı adları değiştirilmelidir. Ağ altyapısındaki cihazlar ağ üzerinden yönetilebilir olmalıdır. Yönetimsel erişimlerde komut satırına, konsol erişimine parola ile giriş sağlanmalıdır. Güvenli protokoller ile yönetimsel işlemler gerçekleştirilmelidir.
- Tüm ağ cihazlarında güvenlikle ilgili güncellemelerin üretici tarafından yayımlanan kararlı ve güncel sürümü kullanılmalıdır.
- Kurum ağ sınırlarından sadece izin verilen kaynaklardan izin verilen hedeflere, izin verilen port ve protokoller ile trafiğin akışı sağlanmalıdır.
- Kablolu ve kablosuz ağlar, bilgi güvenliği gereksinimleri doğrultusunda katmanlara

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

AĞ VE SİSTEM GÜVENLİĞİ YÖNETİM PROSEDÜRÜ

Doküman No	BGYS-PR14
Yayın Tarihi	06.07.2015
Revizyon Tarihi	13.03.2023
Revizyon No	02
Sayfa No	10 / 21

ayrılmalıdır. Yalnızca yetkili sistemlerin, belirli sorumluluklarını yerine getirmek amacıyla gerekli diğer sistemlerle iletişim kurabilmelerini sağlamak için oluşturulan LAN/VLAN'lar arasında erişim denetimi yapılmalıdır. İstemcilerin yer aldığı ağlar ile sunucu/uygulamaların yer aldığı ağlar ayrılmalıdır. Sunucu ağında istemci yer almamalıdır. Yönetimsel işlemler için ayrı yönetim ağları kullanılmalıdır.

- Kurumun internete açık hizmetleri için olası DoS/DDoS saldırılarına karşı servis dışı kalmasını önlemek, iş sürekliliğini sağlamak amacıyla en az aşağıdaki önlemler alınmalıdır.
 - Güvenlik ürünleri üzerinde DoS/DDoS saldırılarına özel konfigürasyonların yapılması
 - DDoS engelleme sistemlerinin sınırları ve yeteneklerinin düzenli aralıklarla test edilmesi ve sürekli iyileştirilmesi/güncellenmesi
 - DDoS koruma için bir servis sağlayıcıdan hizmet temin edilmiş ise; servis sağlayıcıdan yukarıdaki şartlara göre hizmet verildiğine dair taahhüt alınması, tedarik şartname ve sözleşmelerinde bu hususların belirtilmesi.
- Kurum ağına bağlı yetkili kablosuz erişim noktalarının envanteri tutulmalı ve güncelliği sağlanmalıdır.
- Kurum ağı ile fiziksel ve/veya mantıksal olarak izole edilmiş bir misafir ağı oluşturulmalıdır. Misafirlerin, misafir ağına bağlanmaları öncesinde kimlik bilgilerini doğrulayan mekanizmalar devreye alınmalı ve misafirler tarafından misafir ağı üzerinden yapılan tüm erişimler kayıt altına alınmalıdır. Misafir cihazlarının yalnızca misafir ağına erişimleri mümkün kılınmalıdır.
- IP telefon kullanılması durumunda ilgili sistem, altyapı sağlayıcısı veya kurum tarafından güvenlik duvarları ile korunmalıdır.
- IP telefon sistemlerinin iz kayıtları tutulmalıdır. İlgili kayıtlar düzenli aralıklarla bir sunucuda yedeklenmelidir.
- IP telefon sisteminde kullanılacak parolalar güçlü olmalı ve periyodik olarak güncellenmelidir.
- IP telefon sistemlerinde erişim kontrol listeleri kullanılmalı ve kimlik sahteciliği

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

AĞ VE SİSTEM GÜVENLİĞİ YÖNETİM PROSEDÜRÜ

Doküman No	BGYS-PR14
Yayın Tarihi	06.07.2015
Revizyon Tarihi	13.03.2023
Revizyon No	02
Sayfa No	11 / 21

saldırılarına karşı önlem alınmalıdır.

- Kurum ağ cihazlarına ait güvenlik yapılandırmaları; ağ trafiğini düzenleyen kurallara ait tanımlar, kullanılma amacı ve kuralı tanımlayan kişi bilgisi yer alacak şekilde kayıt altına alınmalı ve güncelliği sağlanmalıdır.
- Kurum tarafından gerekli görülen durumlarda, belirlenen kaynak(lar) ve hedef(ler) arasındaki tüm ağ trafiğinin izlenebilmesi için (pcap vb. formatlarda tüm ağ paketlerinin alınabilmesi) kayıt mekanizmaları oluşturulmalıdır. İhtiyaç duyulması durumunda (güvenlik ihlali, şüpheli ağ trafiği vb.) bu mekanizmalar kullanılarak kurum tarafından belirlenen zaman aralığında ilgili trafik kaydı incelenebilmelidir.
- Ağ sınır cihazlarındaki bağlantı trafiği, kullanıcı işlemleri gibi bilgiler kayıt altına alınmalıdır.
- Saldırıları tespit etmek ve engellemek için ağ tabanlı saldırı tespit ve engelleme sistemleri kullanılmalıdır.
- İnternette gelen veya internete giden tüm ağ trafiği, yetkisiz bağlantıları engellemek için uygulama katmanında filtreleme ve kimlik doğrulaması yapılarak iletilmelidir.
- Kurumdaki sistemlerin, kurum tarafından onaylanmayan ve mevzuat gereği erişimi yasak olan web sitelerine bağlanmasını engelleyen ağ tabanlı URL filtreleri uygulanmalıdır.
- URL sınıflandırma servisleri kullanılmalıdır. Bu servislerin kullandığı listeler güncel tutulmalıdır. Kategorilendirilmemiş siteler varsayılan olarak engellenmelidir.
- Potansiyel olarak zararlı etkinlikleri tanımlamak ve saldırıya uğramış sistemlerin belirlenmesine yardımcı olmak için sistemlerden gelen tüm isteklere ait URL'ler kaydedilmelidir.
- Eşler arası (Peer to Peer) kablosuz ağ erişimine olanak sağlayan yöntemler (ad hoc yöntemi vb.) engellenmelidir.
- Kurum ağının uygulama seviyesi saldırılara karşı korunması için gerekli yapılar (WAF, IPS, DDoS vb.) uygun şekilde konumlandırılmalı, test edilmeli ve sürekli iyileştirilmelidir. Bu amaçla bir servis sağlayıcıdan hizmet temin edilmiş ise; servis sağlayıcıdan yukarıdaki

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

AĞ VE SİSTEM GÜVENLİĞİ YÖNETİM PROSEDÜRÜ

Doküman No	BGYS-PR14
Yayın Tarihi	06.07.2015
Revizyon Tarihi	13.03.2023
Revizyon No	02
Sayfa No	12 / 21

şartlara göre hizmet verildiğine dair taahhüt alınmalı, tedarik şartname ve sözleşmelerinde bu hususlar belirtilmelidir.

12. VERİ SIZINTISI ÖNLEME

- Bulut servisleri kullanımı durumunda veri erişimi, muhafazası, kullanımı kapsamındaki güvenlik hususları servis şartname ve sözleşmelerinde belirtilmelidir.
- Kurum bünyesinde veya dışında, kurumun teknoloji sistemleri tarafından depolanan, işlenen veya iletilen tüm kritik verinin envanteri tutulmalıdır.
- Kurum tarafından düzenli olarak erişilmeyen kritik veri veya sistemler ağdan çıkarılmalıdır. Bu sistemler ihtiyaç duyulmadığı durumlarda ağ bağlantısı kesilmiş olarak tutulmalıdır.
- İş ihtiyaçları gereği taşınabilir ortamların kullanılması gerektiği durumlarda, yalnızca kurum tarafından yetkilendirilmiş ve kurum envanterine kayıt edilmiş taşınabilir ortamların kullanılmasına izin verecek şekilde gerekli önlemler alınmalıdır.
- Ağda kritik verinin taşınmasında güvenli protokoller kullanılmalı (VPN teknolojileri, SSL/TLS vb.) ve kritik veri şifreli olarak taşınmalıdır.
- Ağ içerisinde veri akışını kontrol etmek, izlemek ve izinsiz ağ trafiğini takip etmek amacıyla ağ tabanlı veri sızıntısı önleme sistemi kullanılmalıdır.

13. İZ VE DENETİM KAYITLARININ TUTULMASI VE İZLENMESİ

- Tüm sistemlerde ve ağ cihazlarında kayıt mekanizması etkin olmalıdır. Kayıtlar, bilgi güvenliği gereksinimleri ve ilgili mevzuat gereği kabul edilebilir süre boyunca cihaz üzerinde veya harici sistemlerde tutulmalı, yetkisiz erişime ve değişime karşı korunmalıdır. Kayıtlar, muhafazaları için tanımlanan kabul edilebilir sürenin sona ermesi ile birlikte güvenli bir şekilde yok edilmelidir.
- Sistem yöneticisi, operatörler ve kullanıcıların faaliyetleri kayıt altına alınmalı, kayıtlar korunmalı ve düzenli olarak gözden geçirilmelidir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

AĞ VE SİSTEM GÜVENLİĞİ YÖNETİM PROSEDÜRÜ

Doküman No	BGYS-PR14
Yayın Tarihi	06.07.2015
Revizyon Tarihi	13.03.2023
Revizyon No	02
Sayfa No	13 / 21

- Kayıtlarda zaman damgalarının tutarlı olması için ağa bağlı tüm sistemlerin (sunucular, iş istasyonları, güvenlik ürünleri, ağ aygıtları vb.) düzenli olarak zaman bilgisinin alındığı; yedekli yapıda ve senkronize zaman sunucusu kullanılmalıdır.
- Sistem iz kayıtları; olay açıklaması, olay kaynağı, olay zamanı, kullanıcı/sistem bilgisi, kaynak adresleri, hedef adresleri ve işlem detayları bilgilerini içerecek şekilde tutulmalı ve bütünlüğü zaman damgası ile korunmalıdır.
- Kayıt tutan sistemlerde yeterli depolama alanı tahsis edilmelidir. Depolama alanı doluluk oranı düzenli olarak kontrol edilmelidir.
- Analiz ve inceleme amacıyla kayıtlar merkezi bir kayıt yönetim sisteminde toplanmalı ve düzenli olarak yetkili personel tarafından gözden geçirilmelidir. Kayıt tutma veya gönderme işlemi sırasında hata oluştuğunda uyarı mekanizmaları aktif edilmeli ve izlenmelidir.
- Siber olayların korelasyon kuralları doğrultusunda tespiti ve detaylı analizi için siber tehdit ve olay yönetim sistemleri veya kayıt analizi araçları kullanılmalıdır.
- Aksiyon alınabilecek olayların daha iyi tanımlanabilmesi ve gereksiz olayların elenebilmesi amacıyla siber tehdit ve olay yönetim sistemlerinin yapılandırması düzenli olarak gözden geçirilmelidir. Kayıtlar düzenli olarak izlenmelidir.

14. SANALLAŞTIRMA GÜVENLİĞİ

- Ağ ortamları ve sanal makineler, kurum tarafından belirlenen kriterlere göre güvenilir ve güvenilmeyen bağlantılar arasındaki trafik kısıtlanacak şekilde yapılandırılmalıdır. Bu yapılandırmalar düzenli olarak gözden geçirilmelidir.
- Sanallaştırma sistemleri yönetim arayüzlerine erişim, iş ihtiyaçları doğrultusunda tanımlanan yetki ile güvenli bir şekilde yapılmalıdır.
- Sanallaştırma ortamları ile birlikte kullanılacak veya kurum bünyesinde müstakil olarak

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

AĞ VE SİSTEM GÜVENLİĞİ YÖNETİM PROSEDÜRÜ

Doküman No	BGYS-PR14
Yayın Tarihi	06.07.2015
Revizyon Tarihi	13.03.2023
Revizyon No	02
Sayfa No	14 / 21

kullanılacak depolama ortamları ile iletişimin güvenliğinin sağlanmasında aşağıdaki hususlar dikkate alınmalıdır. • Ağ dosya paylaşım servisleri, ayrılmış depolama ağlarında veya yönlendirilemeyen ağlarda hizmet vermelidir. • Ağ dosya paylaşım servislerinde, eğer destekleniyorsa trafik şifreli olmalı, uygun kimlik doğrulama protokolleri kullanılarak erişim denetimi yapılmalı ve kayıtlar tutulmalıdır.

- Sanallaştırma ürünlerinin üretici tarafından desteği devam eden ve kararlı sürümleri kullanılmalıdır. Bu ürünlerin güvenliği ile ilgili duyurular takip edilmelidir.
- Kaynaklara yönelik kapasite planlaması sistemi kullanan birimlerin taleplerine göre, ürünlerin yaşam süresinin sona ermesine göre ve geçmiş dönem veri büyüme oranlarına göre yapılmalıdır. Kapasite planları yıllık gözden geçirilmelidir.
- Yaşam döngüsü sona eren makineler kapatılarak ağdan izole edilmelidir. Üzerindeki veriler sunucu sahibinin talebine göre güvenli imha yöntemleri ile silinmelidir veya yedeklenmelidir.
- Kullanılmakta olan işletim sistemleri, iş gereksinimlerini karşılamak için ihtiyaç duyulan bağlantı noktaları, protokoller ve servisleri sağlayacak şekilde sıkılaştırılmalıdır. Zararlı yazılımdan korunma uygulamaları kullanılmalı, dosya bütünlüğünü izleyecek ve kayıt tutacak mekanizmalar devreye alınmalıdır.
- Tüm sanal makine imajlarının bütünlüğünü denetleyecek ve izleyecek mekanizmalar devreye alınmalıdır.
- Sanallaştırma sistemleri yönetim ara yüzlerine erişim, iş ihtiyaçları doğrultusunda tanımlanan yetki ile güvenli bir şekilde yapılmalıdır.
- Sanallaştırma ortamında kendinden imzalı sertifikalar yerine kuruma ait ve yetkili otoriteden alınmış sertifikalar kullanılmalıdır.
- Sanal makineler arasındaki trafik güvenlik kontrollerinden geçirilmeli, olası zararlı trafiğin ağdaki diğer sanal ve fiziksel makinelere ulaşmaması için gerekli önlemler alınmalıdır.
- Farklı güvenlik seviyesinde yer alan ağlarda kullanılan sanal sistemlere ait kaynaklar

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	AĞ VE SİSTEM GÜVENLİĞİ YÖNETİM PROSEDÜRÜ	Doküman No	BGYS-PR14
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	13.03.2023
		Revizyon No	02
		Sayfa No	15 / 21

fiziksel olarak izole edilmelidir.

15. SİBER GÜVENLİK OLAY YÖNETİMİ

- Siber olaylara müdahale planları doğrultusunda Kurumsal SOME Kurulum ve Yönetim Rehberi'ne uygun olarak çalışmalar yürütülmelidir.
- Siber olayların yönetimi aşamalarında görev alacak personelin rol ve sorumlulukları tanımlanmalı, olay müdahale için gerekli teknik alt yapı personele sağlanmalı ve belirlenen personel ilgili taraflara bildirilmelidir. Siber olay yönetimi kapsamında görev alacak personel Kurumsal SOME Kurulum ve Yönetim Rehberi kriterlerine uygun olmalıdır.
- Siber olay bildirimi yapılacak resmi kurumlara ilişkin iletişim bilgileri dokümanı oluşturulmalı ve periyodik olarak gözden geçirilmelidir. İletişim bilgileri dokümanı, iletişim kurulacak konu kapsamında iletişim kurulacak kişileri tanımlamalıdır. USOM ve olası diğer siber tehdit istihbarat kaynaklarından alınan bildirimler doğrultusunda gerekli önlemleri alınmalıdır.
- Siber olaylar ile ilgili bildirim süresi ve rapora yansıtılacak bilgiler USOM tarafından belirlenen kriterler göz önünde bulundurularak belirlenmeli ve standart hale getirilmelidir. Yaşanan siber olaya ilişkin iş ve işlemlerin detaylı bir şekilde anlatıldığı siber olay müdahale raporu, kurum standartlarına göre hazırlanmalı, üst yönetim, USOM ve varsa bağlı olduğu Sektörel SOME'ye iletilmelidir.
- Kurumların siber olay yönetimi kapsamındaki hizmetleri üçüncü taraflardan alması durumunda hizmetin güvenliği garanti altına alınmalıdır.
- SOME personelinin, gerçek dünyadaki tehditlere cevap verme konusundaki yeteneklerini arttırmak için rutin tatbikatlar planlanmalı ve uygulanmalıdır.

16. SIZMA TESTLERİ VE GÜVENLİK DENETİMLERİ

- Kurum bünyesinde sızma testleri ve güvenlik denetimleri yılda en az bir defa olmak üzere düzenli olarak yapılmalıdır.
- Sızma testleri ve güvenlik denetimleri gerçekleştirilmeden önce testi gerçekleştiren taraf

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

AĞ VE SİSTEM GÜVENLİĞİ YÖNETİM PROSEDÜRÜ

Doküman No	BGYS-PR14
Yayın Tarihi	06.07.2015
Revizyon Tarihi	13.03.2023
Revizyon No	02
Sayfa No	16 / 21

ile gizlilik sözleşmeleri imzalanmalıdır. Hizmet öncesi sızma testi ve güvenlik denetimi kapsamı ilgili şartnamede belirlenmelidir.

- Sızma testleri; farklı yetki seviyelerinde olmak üzere son kullanıcı, standart kullanıcı, admin profillerini içerecek şekilde yapılmalıdır.
- Operasyonel ortamda olup sızma testi yapılması mümkün olmayan veya yüksek risk içeren sistemler için güvenlik denetimleri ve güvenlik sıkılaştırmaları düzenli olarak yapılmalıdır.
- Sızma testini gerçekleştirmek için kullanılan herhangi bir kullanıcı veya sistem hesabı, yalnızca meşru amaçlar için kullanıldığından emin olmak için kontrol edilmeli, izlenmeli, kayıt altına alınmalı ve test bittikten sonra pasif hale getirilmelidir.
- Kapatılan güvenlik açıklarının doğrulama testleri yapılmalıdır.
- Sızma testi ve güvenlik denetimi bulguları karşılaştırılabilir bir puanlama yöntemi dikkate alınarak raporlanmalıdır.
- Canlı ortamda olup sızma testi yapılması mümkün olmayan ve/veya yüksek risk içeren sistemler için gerçeğine benzer test ortamları oluşturulmalıdır.

17. KİMLİK DOĞRULAMA VE ERİŞİM YÖNETİMİ

- Her kullanıcı için kendine ait ve kendisini benzersiz olarak tanımlayan bir kullanıcı hesabı tanımlanmalı, tüm kullanıcı hesaplarına ait bir parola ataması yapılmalıdır. Kullanıcı hesaplarına ait parolalar belirlenirken dikkat edilmesi gereken kurallar tanımlanmalı ve uygulanmalıdır.
- Oturum açma mekanizmasına yapılacak saldırıları engellemek amacıyla uygun güvenlik önlemleri (istek sınırlandırma, IP bloklama, CAPTCHA vb.) alınmalıdır. Başarısız oturum açma denemeleri kayıt altına alınmalıdır.
- Kurum bilgi sistemindeki herhangi bir varlıkta varsayılan kullanıcı adı ve parolalar kullanılmamalıdır. Test ortamlarında kullanımda olan tüm varsayılan kullanıcılar ve

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

AĞ VE SİSTEM GÜVENLİĞİ YÖNETİM PROSEDÜRÜ

Doküman No	BGYS-PR14
Yayın Tarihi	06.07.2015
Revizyon Tarihi	13.03.2023
Revizyon No	02
Sayfa No	17 / 21

parolalar, canlıya alınmadan önce silinmeli veya değiştirilmelidir.

- Sistem yöneticilerinin yüksek haklar gerektiren işlemleri yapmak için ayrı bir hesapları olmalıdır. Yönetici hesaplarıyla yapılan işlemler için denetim kayıtları oluşturulmalıdır. İşlem yapılmayan oturumlar belirli bir süre sonra sonlandırılmalıdır. Kurum kaynaklarına erişimlerde kimlik doğrulama mekanizmaları kullanılmalıdır.
- Sistem yöneticilerinin ve kullanıcılarının yetkileri düzenli olarak gözden geçirilmeli, görev değişikliklerinde erişim yetkileri güncellenmelidir. Bir personelin veya yüklenicinin sorumluluklarının değişmesinden hemen sonra hesapları devre dışı bırakmak ve sistem erişimini iptal etmek için süreç oluşturulmalı ve uygulanmalıdır. Bu hesaplar devre dışı bırakılmalıdır.
- Kurumdaki sistemler bir yönetici hesabı oluşturulduğunda veya silindiğinde kayıt tutacak ve alarm oluşturacak şekilde yapılandırılmalıdır. Tüm yönetici hesap erişimleri için şifreli kanallar kullanılmalıdır. Kurumdaki sistemler bir yönetici hesabından giriş denemesi yapıldığında kayıt tutmakta ve giriş denemesi yapılması durumunda alarm oluşturmalıdır.
- Betik dosyası oluşturma araçlarına (PowerShell ve Python gibi) erişim, yalnızca iş amaçları doğrultusunda bu özelliklere erişmesi gereken hesaplar ile sınırlandırılmalıdır.
- Kimlik doğrulama merkezi olarak yapılmalıdır. Merkezi kimlik yönetim ve doğrulama sisteminin kullanılmadığı durumlarda, risk analizi çalışması doğrultusunda telafi edici önlemler alınmalıdır.
- Tüm kimlik doğrulama bilgileri güçlü kriptografik algoritmalar kullanılarak saklanmalı ve şifreli kanallar kullanılarak iletilmelidir.
- Servis hesapları en az yetki prensibi göz önünde bulundurularak oluşturulmalıdır. Kullanıcı veya yetkili hesaplar servis hesabı olarak kullanılmamalıdır. Servis hesaplarının kurum içerisinde bir sahibi olmalı ve periyodik olarak gözden geçirilmelidir.

18. FELAKET KURTARMA VE İŞ SÜREKLİLİĞİ YÖNETİMİ

- Kurum bünyesinde iş süreçlerinde kullanılan ve iş süreçlerini destekleyen tüm sistemler

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

AĞ VE SİSTEM GÜVENLİĞİ YÖNETİM PROSEDÜRÜ

Doküman No	BGYS-PR14
Yayın Tarihi	06.07.2015
Revizyon Tarihi	13.03.2023
Revizyon No	02
Sayfa No	18 / 21

göz önünde bulundurularak yedekleme ihtiyacı olan sistemler tespit edilmeli ve dokümanite edilmiş bir yedekleme planı üzerinden yedekleme yönetimi yapılmalıdır. Yedekleme planı en az aşağıdaki başlıkları içerecek şekilde oluşturulmalıdır: • Yedeği alınan sistemler • Yedekleme işleminin adı • Yedekleme işlemi başlangıç tarih ve saat bilgisi • Yedekleme tipi • Yedekleme periyodu • Yedekleme süreçlerinde versiyonlama

- Yedekleme planı, yedekleme ihtiyaçları göz önünde bulundurularak yılda en az bir kere gözden geçirilmelidir. Bu gözden geçirme kapsamında iş birimleri ile de görüşülerek yedekleme ihtiyacı ortadan kalkan sistemler tespit edilmeli, yedekleme işleminden çıkarılmalı ve yedekleme işleminde olmayan fakat dâhil edilmesi gereken sistemler tespit edilerek yedekleme işlemine dâhil edilmelidir.
- Yedekleme işlemlerine ilişkin iz kayıtları oluşturulmalı, bu kayıtlar bilgi güvenliği gereklilikleri ve ilgili mevzuat göz önünde bulundurularak tanımlanmış süre kadar tutulmalı ve zaman damgası ile korunmalıdır.
- Yedekleme ortamlarının çalıştığından ve geri dönülebilir olduğundan emin olmak adına; kapsamdaki sistemlerin, uygulamaların ve verinin yedekleri düzenli olarak geri dönüş testlerine tabi tutulmalı ve gerçekleştirilen geri dönüş testlerine yönelik kayıtlar oluşturulmalıdır. Bu kayıtlar en az aşağıdaki bilgileri içermelidir: • Testin gerçekleştirildiği gün ve saat bilgisi • Testi yapılan sistemler • Testin gerçekleştirildiğini kanıtlayan ekran görüntüleri • Testin başarılı sonuçlanıp sonuçlanmadığı • Test sırasında karşılaşılan sorunlar ve çıkarılan dersler
- Yedekleme medyalarının envanteri tutulmalı ve envanter periyodik olarak gözden geçirilmelidir. Yedekleme medyaları, fiziksel olarak güvenli ve yedek alınan bölgeden farklı bir konumda saklanmalıdır. Yedeklenen verinin; ana sistemlerin bulunduğu ortamlar benzer riskleri içermeyen başka bir ortamda saklandığı teyit edilmelidir. Yedeklenen veri tesis/yerleşke dışına taşınırken güvenliğinin sağlandığı ve bulunduğu ortamın fiziksel ve mantıksal güvenliğinin sağlanmış olduğu teyit edilmelidir. Yedekler kullanım süresinin sona ermesi sonrasında ulusal/uluslararası standartlara uygun olarak güvenli bir şekilde

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

AĞ VE SİSTEM GÜVENLİĞİ YÖNETİM PROSEDÜRÜ

Doküman No	BGYS-PR14
Yayın Tarihi	06.07.2015
Revizyon Tarihi	13.03.2023
Revizyon No	02
Sayfa No	19 / 21

imha edilmeli ve imha kayıtları tutulmalıdır.

- Süreklilik yönetimi dâhilinde tüm planlar kurum tarafından belirlenen periyotlarda test edilmeli ve test sonuçları kayıt altına alınmalıdır.
- Süreklilik yönetimi dâhilindeki planların, acil durum müdahale prosedürlerinin ve gerekli diğer dokümanların güncel versiyonlarının kurumun yerleşkesi içinde ve mümkünse kurum binası dışında belirlenecek bir yerde tutulması ve her türlü felaket senaryosu sırasında erişilebilir olması sağlanmalıdır.
- Felaket kurtarma planlarının devreye alınması aşamasında yer alacak tüm paydaşların ve süreç içinde yer alacak personelin görev ve sorumlulukları dokümante edilmeli ve ilgili taraflara bildirilmelidir. Felaket kurtarma planları kapsamında; hizmet alınan üçüncü tarafların rol ve sorumlulukları ile tedarik edilen hizmetlerin sürekliliği dikkate alınmalıdır. Felaket kurtarma çalışmaları dâhilindeki tüm planlar yılda en az bir kez test edilmeli ve test sonuçları kayıt altına alınmalıdır.
- Felaket kurtarma çalışmaları dâhilindeki planların güncel versiyonları her türlü felaket senaryosu sırasında erişilebilir olmalıdır.

19. UZAKTAN BAĞLANTIYLA ÇALIŞMA

- İnternet ortamından kurum içi kaynaklara kontrol dışı erişim engellenmelidir. İnternet ortamından kurum içi kaynaklara erişim gerekli ise VPN teknolojileri kullanılmalıdır.
- Uzaktan bağlantı ile şifrelenmiş bir şekilde akredite edilen kişiler tarafından VPN bağlantısı yapılmalıdır. Bu işlemler için SSL-VPN cihazları kullanılmalıdır. Tek seferde bağlantı süresi 1 saati geçmemelidir.
- Kurum dışı paydaşların kurum kaynaklarına uzaktan erişimine, ilgili kurum personelinin onayı dışında izin verilmemelidir. Uzaktan erişimin gerçekleştiği durumlarda ise aşağıdaki kurallar uygulanmalıdır:
 - Erişim yetkisi sınırlı ve belirli bir süreyle tanımlanmalıdır. Oturum zaman aşımı süresi belirlenmeli ve süre sonunda kullanıcı kimlik doğrulamaya zorlanmalıdır.
 - Çok faktörlü kimlik doğrulama metotları aktif edilmelidir.
 - Erişimin

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

AĞ VE SİSTEM GÜVENLİĞİ YÖNETİM PROSEDÜRÜ

Doküman No	BGYS-PR14
Yayın Tarihi	06.07.2015
Revizyon Tarihi	13.03.2023
Revizyon No	02
Sayfa No	20 / 21

gerçekleştiği hedefler ile erişimin yapıldığı kaynaklar için kısıtlama yapılmalıdır. • Erişimlere ilişkin iz kayıtları tutulmalıdır. • Herhangi bir anomali ve ihlal durumuna karşın gerekli izleme ve alarm mekanizmaları aktifleştirilmelidir. • Erişim yolu şifreli ve güvenli olmalıdır.

20. İŞLETİM SİSTEMİ SIKILAŞTIRMA TEDBİRLERİ

- Kullanılmakta olan işletim sistemleri, iş gereksinimlerini karşılamak için ihtiyaç duyulan bağlantı noktaları, protokoller ve servisleri sağlayacak şekilde sıkılaştırılmalıdır. Zararlı yazılımdan korunma uygulamaları kullanılmalı, dosya bütünlüğünü izleyecek ve kayıt tutacak mekanizmalar devreye alınmalıdır.
- Şifresiz kimlik doğrulama ve haberleşme kullanan servisler (Telnet, FTP, rlogin, HTTP, SMTP vb.), eğer varsa şifreli haberleşme imkânı sağlayan muadilleri (SSH, SFTP, HTTPS, SMTPS vb.) ile değiştirilmelidir

21. WEB ERİŞİM YETKİLERİ

- Kullanıcıların web erişim yetkileri web filtreleme sunucuları ile düzenlenmelidir. Kullanıcıların erişmek istedikleri web sayfalarını e-posta/resmi yazı üzerinden talep etmeleri, birim amirlerinin de bu talebi onaylaması üzerine talep incelemeye alınmalıdır. Bilgi Güvenliği Politikasına aykırı bir durum olmadığı takdirde talep yerine getirilmelidir.

22. SAAY SENKRONİZASYONU

- Saat senkronizasyonu lokalde kurulu olan bir NTP(Ağ Zaman Protokolü) sunucusu ve bir network cihazı(router) ile otomatik olarak yapılmaktadır.

23. GENEL SIKILAŞTIRMA TEDBİRLERİ

- Sunucuların normal işleyişi için gerekli olmayan tüm servisler kapatılmalıdır. Sistemlerde çalışan servisler ihtiyaçları olan en az yetki ile çalışmalıdır. Servis kullanıcılarının yetkileri ayrıca kısıtlanmalıdır. Servislerin döndüğü başlık bilgileri (banner) bilgi ifşasına yol açmayacak şekilde değiştirilmelidir.
- Güncel ve güvenlik desteği devam eden işletim sistemleri kullanılmalıdır. Uygulama

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

AĞ VE SİSTEM GÜVENLİĞİ YÖNETİM PROSEDÜRÜ

Doküman No	BGYS-PR14
Yayın Tarihi	06.07.2015
Revizyon Tarihi	13.03.2023
Revizyon No	02
Sayfa No	21 / 21

sürümleri periyodik olarak kontrol edilmelidir.

- Tüm sunucularda kullanılmayan kablosuz ağ arayüzleri pasif hale getirilmelidir.
- Sunucularda ilgili NTP ayarlamaları yapılarak tüm sunucularda zaman senkronizasyonu sağlanmalıdır.
- İşletim sistemlerinin DEP, ASLR, XD/NX gibi savunma özellikleri istisnai durumlar haricinde aktif olmalıdır. Sistemlerde kullanılmayan uygulamalar belirlenerek kaldırılmalıdır.
- İşletim sistemi güncellemeleri için merkezi bir güncelleme sunucusu oluşturulmalıdır.
- Tüm sunucu ve makinelerde iz kayıtları aktif edilmelidir. Sistem zaman ve tarih ayarları, kullanıcı hesapları, ağ yapılandırması, erişim kontrolleri üzerinde yapılan değişiklikler kayıt altına alınmalıdır. Ayrıca giriş ve çıkış bilgileri, yetkisiz dosya okuma denemeleri, dosya silme işlemleri ve sistem yöneticisi hareketleri de kayıt altına alınmalıdır.
- Sistemlerden syslog vb. araçlarla toplanan sistem iz kayıtları merkezi bir kayıt yönetim sistemine gönderilmelidir. Burada toplanan iz kayıtları kurum kritiklik seviyesi ve dinamiklerine uygun olarak işlenmelidir.
- Tüm makinelerde kullanıcı kimlik doğrulama için merkezi kimlik yönetimi servisi kullanılmalıdır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı

Onaylayan: BGYS Yöneticisi