Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	SEVİNÇ ÇOLAK	DİLEK ÇELİK

1 Amaç

Bu politikanın amacı, sunuculara direkt veya uzaktan yapılan (remote, ssh vb) erişimlerde yetkisiz kullanımdan kaynaklı kritik sistemlerde meydana gelebilecek zararları, hassas bilgilerin kaybını, iş sürekliliğini ve uygulamalardan kaynaklı sistem uygulama yazılımlarından doğabilecek riskleri önlemeye ve azaltmaya yönelik standartları tanımlamaktır.
ESOGÜ BİDB içerisinde bulunan sunucular varlık envanterinde tanımlanmış, ilgili her bir varlık gizlilik, bütünlük ve erişebilirlik olarak sınıflandırılmıştır.

2 Kapsam

ESOGÜ BİDB sunucu sistemleri ve hizmet verdiği projelerin bulunduğu her türlü sistemler kapsam olarak tanımlanmıştır.

3 Tanımlar ve Kısaltmalar

ESOGÜ: Eskişehir Osmangazi Üniversitesi
BİDB: Bilgi İşlem Daire Başkanlığı
Ssh:
UPS: Uninterruptible Power Supply / Kesintisiz Güç Kaynağı
IP: Internet Protocol / İnternet Protokolü
Network Time Protocol (NTP)
DNS
FTP
DEP, ASLR, XD/NX
IPv6
SMTP
SPF, DKIM, DMARC
SSL/TLS sürümleri ile birlikte güvenli e-posta iletişim protokolleri (SMTPs, POP3s, IMAPs, HTTPs vb.) kullanılmalıdır.
SCAP
VMWARE
BGYS: Bilgi Güvenliği Yönetim Sistemi
DMZ: Demilitarized Zone / Sivil Bölge

4 Sorumlular

BİDB Sistem odasındaki dâhili sunucuların yönetiminden Sunucu ve İnternet Sistemleri Birimi sorumludur.

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	SEVİNÇ ÇOLAK	DİLEK ÇELİK

5 Uygulama

- Sunucu sistemlerinde kişisel verilere dair yapılan/yapılacak olan işlemler Kişisel veriler, Kişisel Verilerin Güvenliği Politikası ve Kişisel Verilerin Güvenliği Talimatnamesi doğrultusunda yapılmaktadır.
- Sunucu kurulumları, konfigürasyonları, yedeklemeleri, yamaları, güncellemeleri sorumlu personel tarafından yapılmaktadır.
- Sunucu sistemlerine fiziksel erişim sadece yetkilendirilmiş kişilerce yapılmaktadır.
- Sistem odasında yapılacak her türlü bakım, iyileştirme çalışmaları veya kurulum vb. çalışmalar yetkili personel tarafından veya yetkili personel gözetiminde hizmet alınan kuruluş personeli tarafından yapılmaktadır.
- Sunucu sistemleri ısı seviyesi, kapasite, loglama vb. olarak takip edilmektedir.
- İlgili sunucu sistemleri varlık değerine göre yönetilmektedir.
- Farklı hizmetleri ve farklı kullanıcı grupları olan sunucu rolleri fiziksel veya kavramsal olarak birbirinden ayrılmış durumdadır.
- Sunuculara uzaktan erişim yapılması durumda güçlü kimlik doğrulama yöntemlerine ek olarak ağ yalıtımı da sağlanmıştır.
- Sistem odasında soğutma sistemi, UPS ve yangın dedektörü gibi iş sürekliliğini etkileyecek unsurlar mevcuttur.
- Sunucular üzerinde güncel anti-virüs programları ile çalışmaktadır.
- Sunucular için bir yedekleme politikası tanımlanmış ve minimum (tahammül edilebilir) bilgi kaybına sebep verecek şekilde bir rotasyonlu yedekleme politikası uygulanmaktadır.
- Bütün sunucuların sistem ve veriler yedeklenerek saklanmaktadır.
- Sunucu yedekleri bulunmayan veya yedeklenmeyen sunucuların ise iş sürekliliğini etkilemeyecek, hızlı bir şekilde kurulabilmesi ve ayağa kaldırılması bilgi işlem tarafından sağlanmaktadır.
- Sunucuların gereksiz portları sunucu üzerinde de kapalı şekildedir ve gereksiz servisler pasif veya kurulmamış şekildedir.
- Sunucular daima kritik güncellemeleri alacak şekilde düzenlenmiştir.
- Sunuculara ait IP bilgileri ve diğer önemli bilgiler sadece erişim yetki verilen kişi/kişiler tarafından bilinmektedir.
- Sunucular üzerinde bulunan ve çalışan uygulamaların/servislerin logları tutulmakta ve yaşanabilecek zafiyetlere yönelik belli aralıklarla kontrol edilmektedir
- Sunucu ve sistemlerin saat senkronizasyonu için Network Time Protocol (NTP) alt yapısı kurulmuş ve kullanılmaktadır.

- Sunuculara ait bilgilerin yer aldığı tablo/çizelge ya da platform oluşturulmuş. Burada sunucuların isimleri IP adresleri ve yeri ana görevi ve üzerinde çalışan uygulamalar işletim sistemi sürümleri donanım, kurulum, yedek, yama yönetimi işlemlerinden sorumlu personelin isim ve telefon numaraları bilgisi yer almalı ve bu tablo bir portal üzerinde bulundurulmalıdır. Bilgilerde değişiklik olması durumunda tablo/çizelge (Varlık Envanteri) ya da platform güncellenmektedir.
- ESOGÜ bünyesindeki birimler, Sanal sunucu oluşturulması taleplerini resmi yazı ile BİDB'ye iletilmektedir.
- Kullanılmayan servisler ve uygulamalar kapatılmıştır.
- Sunucu ve altyapı elemanlarının bulunduğu sistem odalarının bakım ve kontrolünde uyulması gereken kurallar "sistem odaları kullanım bakım talimatı " içerisinde belirtilmiştir.
- Sunucular üzerine kesinlikle ticari amaç güden yazılımlar kurulması engellenmiştir.
- Kurumsal uygulamalar (web, DNS, e-posta, FTP vb. ile diğer uygulamalar) ve kurum ağındaki bileşenler, işletim sisteminin ve paket yazılımların kurulumuyla gelen varsayılan güvenlik ayarlarıyla kullanılmakta. Kullanıma alınmadan önce bilgi güvenliği gereksinimleri dikkate alınarak gerekli güvenlik sıkılaştırmaları yapılmaktadır.
- İşletim sistemlerinin DEP, ASLR, XD/NX gibi savunma özellikleri istisnai durumlar haricinde aktif durumdadır.
- Sistemlerde kullanılmayan uygulamalar belirlenerek kaldırılmıştır.
- İşletim sistemi güncellemeleri için merkezi bir güncelleme sunucusu oluşturulmuştur.
- Eğer kurum içerisinde IPv6 kullanılmıyorsa, IPv6 destekleyen tüm sunucularda IPv6 desteği pasif hale getirilmelidir.
- 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 alınmaktadır.
- Sistemlerden syslog vb. araçlarla toplanan sistem iz kayıtları merkezi bir kayıt yönetim sistemine gönderilir. Burada toplanan iz kayıtları kurum kritiklik seviyesi ve dinamiklerine uygun olarak işlenmektedir.
- Sunucuların normal işleyişi için gerekli olan servisler dışında başka bir servisin sunucuda açılması halinde alarm devreye girer ve ilgili servis kapatılılır
- E-posta sunucularında:
  - ✓ Tekrar yayınlama (relay) işlemine, belirlenen IP adresleri dışında izin verilmemeli ve e-posta hizmet protokollerinden kullanılmayanlar kapatılmalıdır.

- ✓ Spam e-postaları engellemek üzere DNS tabanlı filtreleme ve kara liste yöntemleri uygulanmaktadır.
- ✓ E-posta bombardımanı ve bağlantı temelli servis dışı bırakma saldırılarına karşı SMTP sunucusunda bağlantı sayısı sınırlama vb. yöntemler ile koruma sağlanmaktadır.
- ✓ Kurum politikalarına göre gizlilik dereceli bilgi/veri içeren e-posta alışverişleri şifreli ve imzalı olarak yapılmaktadır. E- posta alışverişleri şifreli ve imzalı olarak yapıldığı durumda kullanılan sertifikalar kuruma özel olarak üretilmektedir.
- ✓ 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 edilmetedir.
- ✓ Sahte ya da bütünlüğü bozulmuş e-postaların geçerli etki alanlarına sızma ihtimalini azaltmak için SPF, DKIM, DMARC 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, "E-POSTA POLİTİKASI" gereğince engellenmektedir.
- ✓ E-posta sunucuları, varsayılan ayarlarıyla kullanılmamakta olup kullanıma alınmadan önce tüm sunucuların güvenlik sıkılaştırmaları yapılmaktadır.
- ✓ 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.) kullanılmaktadır.
- ✓ E-posta sunucularına uzaktan yapılacak erişimlerde çok faktörlü kimlik doğrulama mekanizmaları kullanılmakta, ssh ile bağlanılarak güçlü parola politikası uygulanmaktadır.
- ✓ Kuruma dışarıdan gelen e-posta ekleri çok katmanlı güvenlik analizinden (içerik analizi, beyaz liste/kara liste, imza tabanlı anti-virüs, anti-malware taramaları vb.) geçirilmektedir. Bu aşamadan sonra hala kategorilendirilmemiş e-posta ekleri kum havuzunda çalıştırılmakta Kum havuzu çözümlerinde dosyalar yurt içinde yerleşik olan sunucularda taraması yapılmaktadır.
- ✓ Tekrar yayınlama (relay) işlemine, belirlenen IP adresleri dışında izin verilmez ve e-posta hizmet protokollerinden kullanılmayanlar kapalı tutulur.
- ✓ Sahte ya da bütünlüğü bozulmuş e-postaların geçerli etki alanlarına sızma ihtimalini azaltmak için SPF, DKIM vb. teknoloji ve standartlar kullanılmaktadır.
- ✓ E-posta istemcilerinde sadece kurum tarafından izin verilen betik kodları çalıştırılmaktadır.

5.1 Sızma Testleri:

- ESOGÜ BİDB sistemlerinde yılda en az 1 kez dış bir kurumdan/firmadan sızma testi ile sunucuların ve ağ sisteminin zafiyeti test edilmekte ve incelenmektedir.
- ESOGÜ BİDB sistemlerinde kurumda görevli siber güvenlik personeli tarafından periyodik olarak sızma testi ile sunucuların ve ağ sisteminin zafiyeti test edilir ve incelenir
- Kurum ağında yer alan tüm sistemler (test sistemleri de dâhil olmak üzere) güvenlik içeriği otomasyon protokolü (SCAP) uyumlu güvenlik zafiyeti tarama aracı kullanılarak periyodik olarak taranması yapılır.
- Güvenlik taramaları için oluşturulan hesaplar farklı bir amaç için kullanılmaz, en az yetki ve bilmesi gereken prensibi doğrultusunda yetkilendirme yapılarak ilgili erişim kayıtları tutulur.
- Güvenlik taramaları için oluşturulan hesaplar düzenli olarak kontrol edilir ve izlenir.
- Zafiyet tarama araçları, güvenlik açıklarına yönelik yapılan doğrulama faaliyetleri öncesi ve sonrası durumu içerecek şekilde raporlama yapılır.
- Üretilen raporların güvenliği sağlanır ve raporlara sadece yetkili personel erişim mevcuttur.
- Zaafiyet taramaları haftalık olarak yapılmakta olup zaafiyet iç taramaları test sonuçları haftalık raporlanır. Bunun için "PL.03-FR.02- ZAAFİYET TARAMA RAPORU FORMU" kayıt altına alınır. Bu formda yer alan Kritiklik Seviyesi aşağıdaki gibidir.
    - Düşük
    - Orta
    - Yüksek

5.2 Sanallaştırma:

- Sanallaştırma ürünlerinin üretici tarafından desteği devam eden ve kararlı sürümleri kullanılır. Bu ürünlerin güvenliği ile ilgili duyurular takip edilir (VMWARE).
- Gelecekteki ihtiyaçlar, yasal yükümlülükler ve olası güvenlik riskleri göz önünde bulundurularak sistem kaynaklarının planlaması yapılır ve kaynaklar sürekli izlenir. Kapasite artırımı için kurumsal eşik değerleri tanımlanmıştır (PR.15-FR.04 KAPASİTE PLANI).
- Sanallaştırma ortamında kullanılmayan sanal makineler kapatılır, ağdan izole edilir ve sanal makine görev ömrünü tamamlayınca üzerinde yer alan veriler güvenli silme yöntemleri ile imha edilir.
- Kullanılmakta olan işletim sistemleri, iş gereksinimlerini karşılamak için ihtiyaç duyulan bağlantı noktaları, protokoller ve servisleri sağlayacak şekilde sıkılaştırılır. Zararlı yazılımdan korunma uygulamaları kullanılmakta olup, dosya bütünlüğünü izleyecek ve kayıt tutacak mekanizmalar devreye alınmaktadır

- Tüm sanal makine imajlarının bütünlüğünü denetleyecek ve izleyecek mekanizmalar devreye alınmıştır.
- Ağ ortamları ve sanal makineler, kurum tarafından belirlenen kriterlere göre güvenilir ve güvenilmeyen bağlantılar arasındaki trafik kısıtlanacak şekilde yapılandırılmıştır. Bu yapılandırmalar düzenli olarak gözden geçirilir; izin verilen tüm servisler, protokoller, portlar dokümante edilmiş ve kullanım gerekçesi gösterilmektedir (Firewall).
- Sanallaştırma sistemleri yönetim arayüzlerine erişim, iş ihtiyaçları doğrultusunda tanımlanan yetki ile güvenli bir şekilde yapılmaktadır.
- Sanallaştırma ortamları ile birlikte kullanılacak veya kurum bünyesinde müstakil olarak kullanılacak depolama ortamları ile iletişimin güvenliğinin sağlanmasında aşağıdaki hususlar dikkate alınmaktadır. Ağ dosya paylaşım servisleri, ayrılmış depolama ağlarında veya yönlendirilemeyen ağlarda hizmet vermektedir Ağ dosya paylaşım servislerinde, eğer destekleniyorsa trafik şifreli, uygun kimlik doğrulama protokolleri kullanılarak erişim denetimi yapılmakta ve kayıtlar tutulmaktadır.
- Farklı güvenlik seviyesinde yer alan ağlarda kullanılan sanal sistemlere ait kaynaklar fiziksel olarak izole edilmiştir.
- Sunuculara erişimi tanımlayan yetki matrisi oluşturulmuş ve belirli aralıklarla güncellenmektedir. Yetkilendirilen personel sadece yetkilendirildiği kaynaklara erişebilir ve bunları kullanabilmelidir.

5.3 Güvenlik Duvarı:

- Tüm sunucu ve istemcilerde yerel güvenlik duvarı yapılandırılmıştır. Bu yapılandırma en az yetki prensibi göz önüne alınarak yapılmakta. Yapılandırma varsayılan reddetme (default deny) kuralını içerir. Tüm açık portlara ilişkin güvenlik duvarı kuralları yazılmıştır.

5.4 Linux İşletim Sistemi Sıkılaştırma Tedbirleri:

- Kullanılmayan dosya sistemleri (cramfs, freevxfs, hfs vb.) pasif hale getirilmektedir.
- Sisteme erişecek her kişi için ayrı bir kullanıcı hesabı oluşturulmuş. Oluşturulan kullanıcılar için yetkiler belirlenmiş. Kullanılmayan hesaplar kaldırılmış. Sistem kullanıcılarının kabuğu /sbin/nologin şeklinde olup Root login engellenmiştir. Tüm makinelerde UID değeri 0 olan tek kullanıcı root olmalıdır. Ayrıca aynı isme veya UID değerine sahip kullanıcı veya grup bulunmamaktadır. Servis ve sistem kullanıcıları hariç parolasız kullanıcılar bulunmamaktadır. Sudoers kullanıcıları değişikliklere karşı takip edilir.
- İçeriği değiştiğinde, silindiğinde veya taşındığında sistemin çalışmasını olumsuz yönde etkileyebilecek çalışma dosyalarının, kütüphanelerin ve yapılandırma dosyalarının (SUID ve SGID dosyaları, kayıt dosyaları, cron dosyaları, başlangıç betikleri, /etc/passwd, /etc/shadow vb.)

yetkilendirmeleri amacına uygun şekilde düzenlenmiş ve kurum politikaları doğrultusunda denetlenmektedir. Varsayılan kullanıcı umask değeri en az yetki prensibine göre ayarlanmıştır.

- İşletim sistemi dosyaları ile kullanıcı dosyaları, /home, /root, /boot, /tmp vb. birimler ayrı disk bölümlerinde tutulmaktadır.
- CD/DVD ve USB gibi harici medyanın otomatik olarak mount edilmesini önlemek adına otomatik mount özelliği pasif hale getirilmiş. Ayrıca /tmp dizini gibi mount noktalarında noexec, nodev, nosuid parametreleriyle çalıştırılabilir dosyalar pasif hale getirilmiştir.
- Önemli görülen dosyaların bütünlüğü düzenli olarak kontrol edilmektedir.
- Kullanılan makinelerde önyükleyici (bootloader) parolası belirlenmiş ve zorunlu tutulmaktadır. Ayrıca tek kullanıcı modu için kimlik doğrulaması yapılmaktadır. Boot edilebilir cihazlar listesi kısıtlanmanmış. Kullanılmıyorsa USB, Firewire, Thunderbolt, PCMCIA vb. cihazlar iptal edilmiştir.
- İşletim sistemi üzerinde erişim kontrolü, ilgili servisler (SELinux, AppArmor vb.) kullanılarak zorunlu erişim kontrolü (MAC) modeline göre yapılmaktadır.

5.5 Web Sunucusu Sıkılaştırma Tedbirleri:

- Web sunucu yazılımlarının güncel, zafiyet içermeyen ve üreticisi tarafından desteği devam eden kararlı sürümleri kullanılır. Ayrıca, sunucuda kullanımda olan tüm araçların/paket programların güvenlik yamaları için düzenli aralıklarla kontrol yapılmaktadır.
- Web sunucusunun WebDAV (Web Distributed Authoring and Versioning) desteği kaldırılır. WebDAV ile ilgili modüller pasif hale getirilir.
- Web sunucu yazılımı yönetici hesabıyla değil, bu amaç için özel olarak oluşturulmuş bir hesap ile çalıştırılmakta. Web sunucusunda bulunan varsayılan hesaplar/parolalar kullanım dışı bırakılmıştır.
- Web sunucusu bilgi ifşalarını önleyecek şekilde yapılandırılmış. Varsayılan hata ve kurulum sayfaları kaldırılmış. Web sunucu teknolojisi hakkında bilgi ifşasına neden olan HTTP başlıkları kaldırılmıştır. Hatalı HTTP isteklerine dönen cevaplarda bilgi ifşasına izin verilmez.
- POST, GET, OPTIONS ve HEAD metotları dışında diğer HTTP metotları desteklenmez. PUT, DELETE, PROPFIND gibi metotlar web servisi için kullanılıyorsa, kullanımlarının sadece web servis ihtiyaçları ile sınırlı olup olmadığı kontrol edilmelidir. Bu metotların dosya yükleme veya silme gibi farklı amaçlarla kullanımı engellenir.
- Dizin listelemesi pasif hale getirilir.
- Web sunucu yazılımı debug (hata ayıklama) modunda çalıştırılmaz.
- Web sunucu yazılımının desteklediği ölçüde, istekler için limitler belirlenmiş.
- Web sunucu yazılımına ilişkin iz kayıtları alınmaktadır.

- Yazma izni olan dizinler belirlenmiş, yazma yetkileri sadece dosya yükleme ihtiyacı olan dizinlere verilmiş. Uygulama üzerinden yüklenen dosyalar için oluşturulmuş dizinlerde çalıştırma izni kaldırılmıştır.
- Sunucu SSL/TLS kullanımına elverişli yapılandırılmış. Bu kapsamda, sunucuda sadece, bilinen zafiyet içermeyen güvenilir sürüme sahip SSL/TLS versiyonları kullanılmaktadır.
- Web sunucusundaki herhangi bir HTTP bağlantı noktası, şifreleme kullanan bir sunucu bağlantı noktasına yönlendirmiştir.
- Sunucuda sadece kullanılan modüllerin aktif olmalıdır.
- Web sunucusu yalnızca yetkili bağlantı noktalarındaki ağ bağlantılarını dinlemelidir. Kullanımda olmayan portlar kapatılmıştır.
- Uygulama seviyesinde yapılabilecek servis dışı bırakma saldırılarına karşı aşağıdaki sunucu üzerinde aşağıdaki sıkılaştırmalar yapılmalıdır: Sunucunun kabul edebileceği maksimum kullanıcı sayısı artırılmalıdır. Tek bir IP adresinden yapılabilecek bağlantı sayısı sınırlandırılmalıdır. Her bir bağlantının kullanabileceği maksimum ve minimum transfer hızı belirlenmelidir. Bağlantılar için zaman aşım değeri belirlenmeli, belirli bir süre açık kalan bağlantılar sonlandırılmalıdır.
- İnternete açık olarak çalışan web sunucu ayrı bir bölgede (DMZ vb.) tutuluyor.
- Sunucu tarafında koruyucu HTTP başlıkları (X-Frame- Options, Strict-Transport-Security vb.) yapılandırılmıştır.
- Sunucunun özel anahtarına (private key) yapılacak yetkisiz erişimlere karşı önlemler alınmıştır.
- Web sunucularından alınan iz kayıtları merkezi bir kayıt sistemine gönderilmektedir.
- Sunucuya IP adresi üzerinden yapılan erişimler engellenmiştir.

5.6 Sanallaştırma Sunucusu Sıkılaştırma Tedbirleri:

- Sanallaştırma sunucusunda kullanılan sanallaştırma yazılımı güncel ve mevcut güvenlik yamaları yüklenmiştir.
- Konteynerlerin/sanal makinelerin çalıştığı ana makine üzerinde sıkılaştırmalar yapılmıştır.
- Sanal Makineler Arasında Zaman Senkronizasyonunun Sağlanmıştır.
- Sanallaştırma yazılımı ile beraber gelen güvenlik duvarı aktif olmalı ve sadece ihtiyaç duyulan portlar üzerinden ihtiyaç duyulan IP adreslerine erişime izin vermiştir.
- Depolama alanı ağı (SAN) etkinliğini ayırmak için imar ve mantıksal birim numarası (LUN) maskeleme kullanılmaktadır.

- Sanallaştırma ünitelerine erişim sağlayabilen kullanıcıların, sanal makinelerin sahibi olan kullanıcıların ekranlarını yetkisiz olarak görüntülemesi engellenmiştir. Ayrıca yetkisiz konsol erişimleri de engellenmiştir. Her kullanıcı kimlik doğrulaması sonrasında erişim sağlamaktadır.
- Sanallaştırma ünitesinde kullanıcılar en az yetki prensibine uygun şekilde ilgili kullanıcı rollerine atanmıştır.
- Ana bilgisayardan ve sanal makinelerden gerekli olmayan tüm hizmetler/donanımlar kaldırılmıştır. Örneğin, kullanılmayan sanal donanımlar (sürücüler, ağ adaptörleri vb.) devre dışı bırakılmalıdır. Ayrıca gereksiz hipervizör hizmetleri (pano paylaşımı, dosya paylaşımı vb.) devre dışı bırakılmalıdır.
- Sanal disk küçültme (disk shrinking) işleminin sürekli olarak yapılması, sanal diskin kullanılamamasına ve veri kaybına sebebiyet verebileceği için bu ayarı yönetebilecek kullanıcılar belirlenerek, sadece bu kullanıcıların erişimine izin verilmektedir.
- Sanallaştırma yazılımı çalıştığı tüm sunucularda merkezi olarak eş zamanlı güncellenme yapılmaktadır.
- Sanallaştırma ortamında çalışan sanal makineler için alınan iz kayıtları kalıcı bir şekilde saklanır. Ayrıca bu iz kayıtları merkezi bir kayıt sistemine gönderilmektedir.
- Sanal makineler silinmeden önce, sanal makineye ait disk dosyalarına sıfır yazılır ve daha sonrasında kalıcı silme işlemi yapılır.
- Bellek paylaşımı (memory sharing) kullanılmıyor ise devre dışı bırakılmış. Eğer bellek paylaşımı özelliği kullanılacak ise sanal makineler arasında gruplandırma gibi gerekli güvenlik önlemleri alınmıştır.
- Düzenli olarak sunucu sistem yedekleri alınıyor. Yedekler yetkisiz erişime karşı güvenli ortamlarda muhafaza edilmektedir. Belirli aralıklarla yedekten geri dönme testleri gerçekleştirilmektedir.
- Sanal makineye ait imajlar ve anlık görüntüler şifreli olarak muhafaza edilmektedir. Ayrıca, sanal makinelerde disk seviyesinde şifreleme yapılmaktadır.

6 Yaptırım

Bu politikanın ihlal edilmesi durumunda BGYS yöneticisi tarafından gerekli personel desteği de alınarak ihlal nedeni incelenir. İhlal kasıtsız olup personelin eğitim vb. bir eksikliğinden kaynaklanıyorsa problemin kaynağını oluşturan eksikliği kapatmak için çalışma yapılır. Personel BGYS Yöneticisi tarafından e-posta üzerinden yazılı olarak uyarılır.

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	SEVİNÇ ÇOLAK	DİLEK ÇELİK

Eğer ihlal işleminin kasıtlı olduğu anlaşılırsa veya kasıtsız olan ihlaller 3'ten fazla tekrar ederse 657 sayılı devlet memurları kanunu ve Üniversite resmi yazısıyla belirtilen ilave yaptırımlar gereğince personel hakkında işlem yapılır.
Tüm çalışanlar, güvenlik ihlali olaylarını ve bu politikanın ihlallerini, Olay İhlal Yönetimi Prosedüründe tanımlanan şekilde en kısa sürede bildirme sorumluluğundadır.

7 İlgili Dokümanlar

PL.03-FR.02- ZAAFİYET TARAMA RAPORU FORMU
PL.08 - E-POSTA POLİTİKASI
PR.12 - OLAY İHLAL YÖNETİM PROSEDÜRÜ
PR.15-TL.02 SİSTEM ODASI KULLANIM VE BAKIM TALİMATI
PR.15-FR.04 KAPASİTE PLANI
PL.17-FR.01 - UYGULAMA SUNUCU ERİŞİMİ YETKİ MATRİSİ FORMU
PL.19 - KİŞİSEL VERİLERİN GÜVENLİĞİ POLİTİKASI
PL.19 -TL.01- KİŞİSEL VERİLERİN GÜVENLİĞİ TALİMATNAMESİ
PL.22 - KİŞİSEL VERİLERİN YEDEKLEME SAKLAMA VE İMHA EDİLMESİ POLİTİKASI