

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ İHLAL OLAYI YÖNETİMİ PROSEDÜRÜ	Doküman No	BGYS-PR04
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	30.03.2023
		Revizyon No	03
		Sayfa No	1 / 6

1. AMAÇ

Bu prosedürün amacı, Gençlik ve Spor Bakanlığı Bilgi İşlem Dairesi Başkanlığı'nın sahibi olduğu bilgi varlıklarının bilerek veya bilmeyerek, kasten veya tesadüfen 3. şahısların eline geçmesi, kısmen veya tamamen durması / tahrip edilmesi durumunda ortaya çıkan olumsuz durumu yönetmek; olası zayıflıkları tespit ederek, zayıflıkları kullanacak tehditlerin sonuçlarını ortadan kaldırmaktır.

2. KAPSAM

Bu prosedür, Gençlik ve Spor Bakanlığı Bilgi İşlem Dairesi Başkanlığı'nda bilgi sistemlerinde tespit edilen ihlal, güvenlik açıkları, zayıflıklar ve güvenlik olaylarının sonuçlarını kapsamaktadır.

3. TANIMLAR VE KISALTMALAR

Kurum	:T.C. Gençlik ve Spor Bakanlığı
BGYS	:Bilgi Güvenliği Yönetim Sistemi
BGYS Yöneticisi	:Bilgi İşlem Dairesi Başkanı
SOME	:Siber Olaylara Müdahale Ekibi
USOM	:Ulusal Siber Olaylara Müdahale Merkezi
YGG	: Yönetimin Gözden Geçirilmesi

4. UYGULAMA

Bilgi güvenliği ihlal olayı tespit edildiğinde, analizi yapılır ve yayılmasını önlemek için alınması gereken acil eylem gerekli ise süreç başlatılır. Olayın ciddiyeti değerlendirilip yasal işlem öngörülmekte ise, ilgili hukuki ya da güvenlik otoriteleri sürece dâhil edilir.

USOM, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi vb. tarafından tespit edilen Bilgi güvenliği ihlal olayları SOME Ekibine iletildiği gibi; USOM'un kendi sitesi üzerinden de SOME Ekipleri tarafından SMS ya da sistem üzerinden bilgilendirme yapılır. Ayrıca Resmi yazı ile bilgilendirmeler gerçekleştirilir. Gelen teknik rapor incelendikten sonra ilgili birimle görüşme yapılır. Hemen müdahale edilecek durumlarda ihlal olayının önü kesilir. Müdahale sonrası oluşturulan rapor üst yazı ile USOM'a gönderilir.

4.1. Sorumluluklar

- Bilgi güvenliği ihlal olayı tespiti konusunda tüm çalışanlar öncelikli ve gerçek sorumludurlar. Bununla birlikte tüm kullanıcılar sistemde oluşan olağan dışı durumları "BGYS-FRM06 İhlal Olayı Formu" nu doldurarak SOME Ekibine bildirmekle sorumludurlar.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ İHLAL OLAYI YÖNETİMİ PROSEDÜRÜ	Doküman No	BGYS-PR04
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	30.03.2023
		Revizyon No	03
		Sayfa No	2 / 6

- BGYS Yöneticisi olayların tespitinden sonraki süreçler olan delil toplama, önlem alma, deneyim edinme ve disiplin yönetimi konularında çalışma gerçekleştirecektir. İhlal olayları ile ilgili oluşturulan kayıtlar bilgi güvenliği toplantılarında BGYS Takımı ile paylaşılacaktır.
- BGYS Takımı tekrar edebilecek ihlal olaylarını engellemek veya gerçekleşmesi durumunda müdahale edebilmek için ihlal olayları ile ilgili oluşturulan kayıtları incelemek ile sorumludur.
- BGYS Yöneticisi olayların tespitinde kendi elde ettiği bilgileri veya başkaları tarafından onay verilen bilgileri alıp, bunların bir bilgi güvenliği ihlal olayı olup olmadığına karar vermekle sorumludur.
- Bilgi güvenliği olaylarına hızlı etkili ve düzenli şekilde cevap verebilmek için bilgi güvenliği ihlal olayları karşısında BGYS Yöneticisi öncelikli ve gerçek sorumludur. Tespiti yapılan olay ile ilgili kurum dışı birim ya da firma / kurumdan destek alınması gereken durumlarda iletişimi kurmak ve sağlamak konusunda öncelikli sorumluluk müdahaleyi yapacak olan ilgili birim amiridir.

4.2. Bilgi Güvenliği İhlal Olayları Yönetimi

4.2.1. Tespit

Kurum çalışanlarının şüpheli buldukları durumlarda acil bir şekilde olay bildirimi yaparak iletişime geçmeleri gereklidir. İstem dışı kaybolan veya ortaya çıkan dosyalar, anti-virüs ajanının çalışmasında çıkan sorunlar, bilgisayarların aşırı yavaşlaması, istemsiz çalışan programlar ve istemsiz açılan pencereler, yetkisiz personelin güvenli alanlarda bulunması, gizli dosyaların dış müdahaleye açık olması gibi çok özel durumlarda da acil bir şekilde olay bildirimi yaparak bilgilendirme yapılır.

SOME Ekibi düzenli bir şekilde aşağıdaki kontrollerin uygulanmasını sağlayarak bir bilgi güvenliği ihlal olayı oluşmasını kontrol etmelidir.

Fiziksel olarak sistem ve servislerde açıklıkların bulunup bulunmadığı kontrol edilmelidir.

- Sistem güvenlik yazılımları
- Erişim Kontrol Politikasına göre erişim denetimi sırasında tespit edilen farklı yetkiler ve kullanıcılar.
- Yazılan prosedürlere göre doğru uygulanmayan işlemler.

BGYS yöneticisi ve BGYS Takımı, birimlerinde tespit ettikleri ve personelden gelen bilgiler içerisinden veya kendi kontrollerinden elde ettikleri veriler ile aşağıdaki maddelerdeki durumlardan birini tespit eder ise bilgi güvenliği ihlal olayı tespit etmiş olur.

☐ Bilişim ve bilgi işlem sistemlerinden bir kısmının kayıp olduğu / çalındığı tespit edildi.	☐ Sunucu sistemlere ve ağ sistemlerine yetkisiz kişilerce erişimde bulunduğu tespit edildi.
---	--

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ İHLAL OLAYI YÖNETİMİ PROSEDÜRÜ	Doküman No	BGYS-PR04
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	30.03.2023
		Revizyon No	03
		Sayfa No	3 / 6

☐ Bilişim ve bilgi işlem sistemlerinden bir kısmının hasar gördüğü tespit edildi.	☐ Lisanssız yazılım kullanıldığı tespit edildi.
☐ Kimlik kartı / elektronik kimlik / OTP vb. kimlik cihazlarının kayıp olduğu / çalındığı tespit edildi.	☐ Sistem yöneticilerinden herhangi birine tahsis edilmiş kullanıcı hesabının (sunucu ve ağ sistemleri şifreleri, vb.) başka kişilerce kullanıldığı tespit edildi.
☐ Sunucularda virüs tespit edildi.	☐ Kurum sistemlerine izinsiz donanım bağlantıları yapıldığı tespit edildi.
☐ Sistem yöneticilerinin kullandığı istemcilerde virüs tespit edildi.	☐ Bilgi Güvenliği Politikası ve Prosedürlerince belirlenen kullanım kurallarının ihlal edildiği tespit edildi.
☐ Gizlilik dereceli belgelerin (basılı / elektronik) kontrolsüz durumda bulunduğu tespit edildi.	☐ Kurum dışına izinsiz olarak donanım çıkartıldığı tespit edildi.
☐ Gizlilik dereceli belgelerin (basılı / elektronik) kontrolsüz olarak kurum dışına çıkarıldığı tespit edildi.	☐ Sunucu sistemler ve ağ sistemler için alınmış bulunan güvenlik önlemlerini etkisiz hale getirecek fiziksel bağlantı değişikliklerinin yapıldığı tespit edildi.
☐ Gizlilik dereceli belgelerin (basılı / elektronik) kaybolduğu veya tahrip edildiği tespit edildi.	☐ Elektronik, görsel veya basılı yayın organlarında veya benzeri halka açık ortamlarda Kurum sistemlerine ilişkin teknik bilgi ve detayların duyurulduğu tespit edildi.
☐ Gizlilik dereceli belgelere (basılı / elektronik) yetki sahibi olmayan taraflarca erişildiği tespit edildi.	☐ Güvenlik Denetiminin Bilgi İşlem Dairesi Başkanlığı dışında başka kişilerce gerçekleştirildiği tespit edildi.
☐ Sunucu sistemler ve ağ sistemlerinde bilgi kaybı olduğu / verilerin yetkisiz olarak değiştirildiği tespit edildi.	☐ Sunucu sistemler ve ağ sistemlerinde işlev ve hizmet kaybı olduğu tespit edildi.

4.2.2. Raporlama ve Değerlendirme

Bilgi güvenliği ihlal olayı tespiti sonrası olayla ilgili deliller toplanmalı ve raporlanmalıdır. Müdahaleden önce kayıtların toplanması, bozulması engellenecek şekilde saklanması ve yetkisiz erişime karşı korunmasından SOME Ekibi sorumludur.

Raporlama müdahale için gerekli bilgileri kapsayacak detayda olmalı ve kayıtlar içermelidir. Olayların önceliklendirilmesi için olayın etkisini, kapsamını ve sınıflandırılmasını belirlemek amacıyla SOME Ekibi verileri incelemelidir.

Kayıtlar ve içeriği hakkında hazırlanması gereken rapor “BGYS-FRM06 İhlal Olayı Formu” doldurularak yapılır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ İHLAL OLAYI YÖNETİMİ PROSEDÜRÜ	Doküman No	BGYS-PR04
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	30.03.2023
		Revizyon No	03
		Sayfa No	4 / 6

Bilgi güvenliği olay raporlama için dikkat edilmesi gereken durumlar şunlardır:

- Fiziksel güvenlik düzenlemeleri ve ortamlardaki giriş bilgileri
- Etkisiz güvenlik kontrolü
- Bilginin gizlilik, bütünlük, erişilebilirlik durumu ihlali
- İnsan hataları
- Kontrolsüz yazılım veya donanım sistem değişiklikleri
- Arızalar
- Erişim kontrolü
- Politika ve prosedürlere uyumsuzluk
- Sistem güvenlik yazılımları tarafından tespit edilen açıklıklar.

Yukarıda bahsedilen başlıklar için açılan kayıtlar Bilgi güvenliği toplantılarında değerlendirilir. İhlal olayları risk değerlendirmesi kapsamında ölçülür. Değerlendirme mekanizması aşağıdaki gibidir.

- Değerlendirmeler yıllık olarak YGG toplantılarında görüşülür.
- İhlal olaylarını değerlendirmede olay sayısı ve olay etkisi göz önünde bulundurulur.
- İhlal olaylarından gelen veriler risk değerlendirmelerinde ölçüm olarak kullanılır.
- Etki değeri bilgi güvenliği toplantılarında görüşülerek, kayıt sayılarına ve kayıtların etkisine göre risk değerlerine yansıtılır.

4.2.3. Müdahale

Kontroller veya bildirilen durumlar ile tespit edilen ve delilleri toplanan tüm olaylar için diğer işlemlerden önce olaya sebep olan zafiyet düzeltilmelidir.

Zafiyetlerin kapatılmasından sonra mutlaka kontroller tekrarlanmalı ve zafiyetin kapandığı onaylanmalıdır. Delilleri tahrip edecek veya bozacak hiçbir açıklık için kapatma işlemi gerçekleştirilmemelidir.

Risk seviyesi çok yüksek olaylar için sistemler tamamen kapatılmalı veya diğer sistemlere erişimi engellenmelidir.

Bilgi güvenliği ihlal olayına yapılan müdahaleler USOM üzerinden takip edilerek olay yönetimi, deneyim edinme ve önlem alma amacıyla kayıt altına alınmalıdır. Gelen ihlal olayları bildirimlerine en kısa sürede delil toplanarak müdahale edilmelidir.

- Olaya müdahale konusunda yeterli yetkinlik bilgi ve beceriye sahip olunmaması durumunda kurum içi veya kurum dışı ilgili çalışan ya da 3. tarafla iletişime geçilmelidir.
- İhlal olayı için işlemlerden önce kanıtlar toplanmalıdır.
- Risk oluşturan varlık en kısa süre içerisinde zarar verebileceği ortamdan uzaklaştırılmalı veya ayrılmalıdır.
- Kontroller sonucunda tespit edilen olaylar için mutlaka belirli bir süre daha benzer kontroller tekrarlanmalıdır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ İHLAL OLAYI YÖNETİMİ PROSEDÜRÜ	Doküman No	BGYS-PR04
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	30.03.2023
		Revizyon No	03
		Sayfa No	5 / 6

- Müdahale esnasında raporlama için gerekli zafiyet analizi, adli analiz, maliyet tespiti ve ihlal sebepleri gibi veriler toplanmalıdır.

4.2.4. Önlem alma ve Deneyim edinme

Tespit edilen, delilleri toplanan ve daha sonra oluşmasına sebep olan açıklıkların kapatılması sonrasında mutlaka her bir olay için tekrar oluşmasını engellemek için önlemler alınmalıdır.

Açıklığı kapatılıp önlem alınmayan veya deneyim edinilmeyen hiçbir bilgi güvenliği ihlal olayı olmamalıdır.

Deneyim edinme herhangi bir ihlal olayının tekrarlanmamasını veya tekrar oluştuğunda soruna daha kısa sürede çözüm bulunmasını amaçlar.

Bir güvenlik ihlal olayına önlem almak için aşağıdaki işlemlerden herhangi biri uygulanabilir. Yapılan işlemler mutlaka kayıt altına alınmalıdır.

- Oluşturulan kayıtlar incelenmeli ve çözüm yolları ve çözümler için gerekli iletişim bilgileri kayıt edilmelidir.
- Yanlış uygulamalardan kaynaklı olaylar için mutlaka yazılı prosedürler oluşturulmalıdır.
- Prosedürlerden kaynaklanan olaylar için prosedürler tekrar gözden geçirilmeli ve düzeltilmelidir.
- Fiziksel açıklıklardan kaynaklı olaylar için fiziksel önlemler veya ek projeler gerçekleştirilmelidir.
- Kurum içerisinde çalışmalar ile çözülmeyecek olaylar için ek projeler yapılmalı ve alımlar gerçekleştirilmelidir.
- Erişim kaynaklı sorunlar için erişimler tekrar denetlenmeli, diğer benzeri erişim yetkileri de kontrol edilmelidir.
- Yazılım ve uygulamalardan kaynaklı olaylarda güncelleştirmeler kontrol edilmeli, açıklıklar güncelleştirme, ek yama geliştirme gibi yöntemler ile kapatılmalıdır.
- Fiziksel teçhizatlardan kaynaklı sorunlar için alınan önlemler tüm diğer benzer teçhizatlarda da uygulanmalıdır.
- Virüs, Trojan veya zararlı kodlardan kaynaklı olaylar için sorun kaynağı tespit edilmeli, güvenlik yazılımlarını niye yeterli olmadığı irdelenmelidir. Bulunan önlemler mutlaka tüm sisteme uygulanmalıdır.

4.2.5. Kayıt ve Kanıt Toplama

Olayın tespiti ve sorumlunun belirleneceği kayıtların bütünlüğünün bozulmadığı kontrol edilmelidir. Bütünlüğü kanıtlanamayan kayıtlar için işlemler yapılmamalıdır.

- Bilgi güvenliği ihlal olayları için toplanan deliller 2 yıl boyunca silinmemelidir.
- Sorumlu tespiti ile ilgili durumlarda kamera varsa mutlaka kamera kayıtları,
- Erişim kayıtları,
- Kontrol kayıtları,

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ İHLAL OLAYI YÖNETİMİ PROSEDÜRÜ	Doküman No	BGYS-PR04
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	30.03.2023
		Revizyon No	03
		Sayfa No	6 / 6

- Sistem güvenlik yazılımları tarafından tutulan kayıtlar,
- Sorunların çözülmesi için gerekli maliyet kayıtları,
- Bilgi güvenliği olaylarının değerlendirilmesi için ihtiyaç gösterebilecek ve gelecekteki olayların sıklığı, hasar ve maliyet sınırlarını belirleyecek kayıtlar.

4.2.6. Disiplin İşlemleri

Deliller toplandıktan sonra sadece BGYS Yöneticisi, SOME Ekibi ve Üst Yönetim tarafından görülmeli ve disiplin sürecine göre başka kişiler ile paylaşılmalıdır. İhlal olayına sebebiyet veren kişiler hakkında BGYS-PR37 Disiplin Prosedürüne göre işlem yapılır.

5. İLGİLİ DOKÜMANLAR

- BGYS-FRM06 İhlal olayı Formu
- BGYS-PR37 Disiplin Prosedürü

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi