BİLGİ GÜVENLİĞİ İHLAL YÖNETİM PROSEDÜRÜ:

Politika Adı:	BİLGİ GÜVENLİĞİ İHLAL YÖNETİM PROSEDÜRÜ
Doküman Kodu:	BGYS.PR.T.008.ATABAUM.IS
Doküman Sahibi:	BGYS Yöneticisi
Doküman Onay Tarihi:	05/12/2021
Gizlilik Sınıfı:	İç Kullanım

İçindekiler:

AMAÇ:

Bu prosedürün amacı, Kuruluş bilgi varlıklarının Gizlilik, Bütünlük ve Erişilebilirliğini bozan Bilgi Güvenliği olaylarının belirlenmesi, kabul edilir sürede düzeltilmesi ve tekrarının önlenmesi için yapılacak çalışmaları tanımlamayı amaçlar.

KAPSAM:

Kurum bilgi, bilgi sistemleri, ilişkili altyapı, Personel ve 2. Taraflar.

TANIMLAR:

SORUMLULAR:

İlgili Sorumluluklar SİBER OLAYLARA MÜDAHALE TABLOSU'nda tanımlanmıştır. Sorumluların ilgili Sistem Yöneticisi olmasına dikkat edilmiştir.

Ancak tabloda uyan tanım mevcut değilse "BGYS Yöneticisi" ile iletişime geçilerek alınacak tedbirler belirlenir, olay kapanışında bu prosedüre ilişkili olay tanımı girilir.

UYGULAMA:

1. Bilgi güvenliği ile ilgili olaylar personel, yetkili personel, 3. kişiler tarafından bildirmesi gerektiği politikalara uygun şekilde işleyerek taraflara bildirilmelidir.
2. Bilgi Güvenliği Olay ve Zayıflık Bildirimi için Kurum, Olay Tipine bağlı olarak aşağıdaki iletişim kanallarını kullanır:
    a. isms@...com E-posta adresi üzerinden
    b. Doğrudan telefon hattı veya iç hat numarası ile ilişkilendirilmiş bir telefon hattı,
    c. Bir web formu.
3. Bilgi Güvenliği İhlali durumunda Genel Müdür ile iletişime geçilecektir.
4. İhlal durumunun bildirilmesinin akabinde takip işleminin yapılabilmesi için "BİLGİ GÜVENLİĞİ İHLAL YÖNETİM FORMU" doldurulur. Olası bir tehdide meydan verecek bir zayıflığı tespit eden taraflar "Zayıflığı Test Etmeden" derhal yukarıdaki yetkililere haber vermelidirler.
5. Öncelikle oluşan her olay alt olaylar ile ilişkilendirilerek aşağıda yer alan (A-N arasında belirtilen) adımlar uygulanır.

6. Bilgi Güvenliği İhlal Durumunda, 5N1K prensibi uygulanarak olay delilleri toplanır. Bilgi Güvenliği Olay Bildirim Formu doldurularak uygunsuzluk açılır.
7. BİLGİ GÜVENLİĞİ OLAYINA BAĞLI DİSİPLİN KARARLARI FORMU'na bağlı olarak;
    a. Ana Etki seviyesine sahip olaylarda ihtar ve eğitim kararları, Bilgi Güvenliği Yöneticisi veya ilgili birim (Departman) Yöneticisi tarafından doğrudan verilir.
    b. 2 Ana Etki seviyesine sahip tüm olaylarda karar Etik Kurul tarafından alınmalıdır. Bilgi Güvenliği Yönetim Sistemine sahip ilgili Etik Kurul, ilgili kişinin birim yöneticisi, İnsan Kaynakları birimi ve Avukattan oluşur. Bilgi Güvenliği Yöneticisinden gelen tutanaklar olay delilleri ve uygunsuzluk raporu doğrultusunda, Avukat görüşü alınarak BİLGİ GÜVENLİĞİ OLAYINA BAĞLI DİSİPLİN KARARLARI FORMU'ndaki kararlar uygulanır.
    c. İlgili olayı gerçekleştiren kişinin kastının olması durumunda kişinin bilgi varlıklarına erişimi derhal kısıtlanır. Bilgi varlıkları fiziksel ve dijital olabilir. Bu karar Avukat onayından geçer.
8. Tüm alınan kararlar yazılı tutanak ile kayıt alınır ve personel özlük dosyasına eklenir.
9. Bilgi varlıklarının Gizlilik, Bütünlük ve Erişilebilirliğini tehdit eden tüm olaylar ile ilişkili Bilgi Varlıkları sahibi ve Risk sahipleri Bilgi Güvenliği olayına yanıt dönülmesi konusunda sorumludur. **ISO 27001:2013. A.16.1.1.**
10. Olası Bilgi Güvenliği İhlal olayları Risk değerlendirme/analiz işlemleri ile değerlendirilerek kontroller uygulanır,
11. Bilgi Güvenliği İhlal olayları kayıt altına alınarak yönetime raporlanır. **ISO 27001:2013, A.16.1.2.**
12. Yönetime raporlanan olaylar, yasal ve teknik gereklilik dikkate alınarak ilgili kuruluşlar ile avukat aracılığı ile iletişime geçilir. Bu kuruluşlar;
    a. Olay bir suç ile ilişkili ise Savcılık,
    b. Bir kişisel veri ile ilişkili olay ise KVKK
    c. Kuruluş borsaya tabi ise SPK,
    d. Kuruluş TR-SOME ile ilişkili ise TR-SOME,
    e. vd.
13. Bilgi Güvenliği açıklıkları/zayıflıkları zaman kaybedilmeden yönetime raporlanır. **ISO 27001:2013, A.16.1.3.**
14. Bilgi Güvenliğini İhlal eden bir olayda İlgili varlık sahibine, risk sahibine zaman kaybedilmeden bildirilir,
15. Bilgi Güvenliği İhlaline, Bilginin Gizlilik, Bütünlük ve Erişilebilirliğini kabul edilir sürede, kabul edilebilir seviyeye getirilmesi için yanıt verilir. **ISO 27001:2013, A.16.1.5.**
16. Bilgi Güvenliği olayı, ilgili varlık ve risk sahiplerinin katılımı ile değerlendirilerek, sınıflandırılmalıdır. **ISO 27001:2013, A.16.1.4.**
17. Bilgi Güvenliği olaylarının tekrar gerçekleşmemesi için Risk değerlendirmesi/analizi gerçekleştirilerek önlemler alınır. **ISO 27001:2013, A.16.1.6.**

A. YETKİSİZ ERİŞİM:

1. Yetkisiz erişim tespiti durumunda yetkisiz erişim gerçekleştirilen sistem, ağ ortamı ile ilişkisi kesilerek incelemeye alınır,
2. Bu inceleme esnasında Adli Bilişim İncelemesinin eksiksiz yapılabilmesi ve veri kaybının önlenmesi için sistemin gücü kesilmez veya yeniden başlatılmaz,
3. Şayet sistem sanal bir ortamda ve kapatılmasına neden olmuyorsa "Snapshot" alınır,
4. Sistem üzerindeki log kayıtlarının tamamı dış bir ortama alınır,
5. Olayın şiddetine ve etkisine göre Adli Bilişim İncelemesi talep edilebilir,
6. Sistem verilerinin (veri tabanları, programlar ve konfigürasyonlar) mevcut yedeği alınır,
7. Sistem logları ve olayın kaynağı incelenir, kaynağın tespit edilmesi durumunda öncelikle var ise sistemin yedeği güvenli hale getirilerek devreye alınır,
8. Erişim yapılan sistemdeki tüm erişim bilgileri (parolalar) güvenli bir ortam üzerinden yenilenmelidir,
9. Sistem zayıflıklara karşı taranmalıdır. Bu noktada saldırganın kullandığı erişim metodu kullanılmalıdır,
10. Olay ile ilgili yasal takibat gereken bir durum olması durumunda yetkili kişiler/makamlar Üst yönetimin onayı ile yazılı olarak bilgilendirilmelidir,
11. Sistem logları en az bir (1) hafta takibe alınarak anormal durumlar takip edilmelidir,
12. Olayın tekrarlamaması için Risk Analizi gerçekleştirilerek uygun kontroller tanımlanmalıdır.

B. ZARARLI YAZILIM AKTİVİTESİ:

1. Zararlı Yazılım Aktivitesi gözlemleyen tarafın bildiriminin akabinde ilgili sistem ağdan ayrılmalı,
2. İlgili Sistemdeki veriler boş bir ortama (yani o ortama da bulaştığında sistemleri ve ortamlar etkilemeyecek ortama) yedeklenmelidir,
3. Sistem log kayıtlarının tamamı alınmalıdır,
4. Zararlı yazılımın tip/tür tanımları belirlenmelidir,
5. Zararlı yazılım ile ilgili bilgiler ve açıklığın belirlenmesinin ardından sistem temizlenmeli veya baştan temiz kurulum yapılmalı,
6. Olay ile ilgili yasal takibat gereken bir durum olması durumunda yetkili kişiler/makamlar Üst yönetimin onayı ile yazılı olarak bilgilendirilmelidir,
7. Olayın tekrarlamaması için Risk Analizi gerçekleştirilerek uygun kontroller tanımlanmalıdır.

C. DONANIM ARIZALARI:

1. Arıza yapan donanımın neden arızalandığı ön-analizden geçirilmelidir;
2. Bu ön-analiz; güç kesilmesi, iklimlendirme, aşırı ısınma, toz, darbe, yıldırım, vb. nedenlerden kaynaklı olup olmadığı belirlenmelidir.
3. Ön-analiz yeni sistem devreye alındığında da arızanın tekrarlanmasına neden olacak ise yedek sistem devreye alınmalı, sistem çalışmaya zorlanmamalıdır,
4. Sistem yedeği mevcut ise devreye alınmalı, mevcut değil ise üreticiden tedarik talep edilmelidir. Bu noktada cihaz bakım, yenileme sözleşmeleri kapsamında kapasite planı dahilinde bir üst sistem değerlendirmesi yapılmalı, arıza tipik ve sistemden kaynaklı ise uygun başka bir sistem tedarikine gidilmelidir,
5. Arıza fiziksel ve kasıt içeriyorsa bileşenlere dokunulmadan tüm erişim kayıtları korunmalıdır (Kamera kayıtları, giriş/çıkış kayıtları), sistem bileşenleri (HDD, vb. ortamlar),

6. Olay ile ilgili yasal takibat gereken bir durum olması durumunda yetkili kişiler/makamlar Üst yönetimin onayı ile yazılı olarak bilgilendirilmelidir,
7. Olayın tekrarlamaması için Risk Analizi gerçekleştirilerek uygun kontroller tanımlanmalıdır.

D. YAZILIM ARIZALARI:

1. Yazılım arızaları, ilgili sistem/servis yöneticisine zaman geçirilmeden bildirilmelidir,
2. Olayın tekrarlamaması için risk analizi gerçekleştirilerek uygun kontroller tanımlanmalıdır.

E. AĞ ARIZALARI:

1. Ağ arızası, arızanın çıktığı konum ve açıklamalar Ağ Yöneticisine zaman kaybedilmeden bildirilmelidir,
2. Ağ arızası ile ilişkili olduğu düşünülen sistem, sistem bileşeni ağa dahil edilmemelidir,
3. Olayın tekrarlamaması için Risk Analizi gerçekleştirilerek uygun kontroller tanımlanmalıdır.

F. VERİ KAYBI:

1. Donanımsal, Yazılımsal Veriye erişememe, Verinin kaza ile silinmesi, Verinin çalınması, Verinin kasıtlı veya kasıtsız şifrelenerek erişilmez duruma getirilmesi durumunda ilgili sistem üzerinde hiçbir işlem yapılmadan, sistem kapatılmadan BGYS Yöneticisine iletilmelidir,
2. Veri kaybı giderilene kadar ilgili sistemlere yeni veri eklenmemeli veya silinmemelidir.
3. Olayın tekrarlamaması için Risk Analizi gerçekleştirilerek uygun kontroller tanımlanmalıdır.

G. HIRSIZLIK:

1. Bir bilgi varlığı olan, Bilgisayar, Taşınabilir Bilgisayar, Cep Telefonu, Tablet, vb. Donanım, Yazılım, CD, HDD, Harddisk, Taşınabilir Disk, Kağıt ortamında her türlü evrak, gibi ortamlar çalındığı anlaşıldığı anda BGYS yöneticisine;
    a. Çalınan bileşen açıklaması (Var ise, Marka/Model, Bulunduğu ortam, vb.)
    b. Çalınan bileşenin seri numarası (Daha önce sistem tarafında ve kullanıcı tarafında tutuluyor olmalıdır)
    c. Çalındığı yer/ortam,
    d. Vaka ile ilgili detaylar, şahit görüşleri yazılı olarak iletilmelidir,
2. Olay ile ilgili yasal takibat gereken bir durum olmasından dolayı yetkili kişiler/makamlar Üst yönetimin onayı ile yazılı olarak bilgilendirilmelidir,
3. Olayın tekrarlamaması için Risk Analizi gerçekleştirilerek uygun kontroller tanımlanmalıdır.

H. KIRILMA:

1. Bir bilgi varlığı olan; Bilgisayar, Taşınabilir Bilgisayar, Cep Telefonu, Tablet, vb. Donanım, Yazılım, CD, HDD, Harddisk, Taşınabilir Disk gibi ortamların kırıldığı anlaşıldığı anda BGYS yöneticisine;
    a. Kırılan bileşenin açıklaması (Var ise, Marka/Model, Bulunduğu ortam, vb.)
    b. Kırılan bileşenin seri numarası (Daha önce sistem tarafında ve kullanıcı tarafında tutuluyor olmalıdır)
    c. Kırıldığı yer/ortam,
    d. Vaka ile ilgili detaylar, şahit görüşleri yazılı olarak iletilmelidir,
    e. Sistem kırık hali ile kullanılmamalıdır. Bilgi varlığının tekrar kullanılabilmesi için ön-kontrolden geçmelidir.

2. Olay ile ilgili yasal takibat gereken bir durum olmasından dolayı yetkili kişiler/makamlar Üst yönetimin onayı ile yazılı olarak bilgilendirilmelidir,
3. Olayın tekrarlamaması için Risk Analizi gerçekleştirilerek uygun kontroller tanımlanmalıdır.

I. UYGUNSUZ DAVRANIŞLAR ve POLİTİKAYA UYMAYAN KİŞİLER:

1. Bilgi varlıklarının Gizlilik, Bütünlük ve Erişilebilirliğini bozabilecek davranışlar ile Mevcut Politika, Prosedür ve Talimatlara uymana kişiler BGYS Yöneticisine zaman kaybedilmeden bildirilmelidir,
2. Olay ile ilgili yasal takibat gereken bir durum olmasından dolayı yetkili kişiler/makamlar Üst yönetimin onayı ile yazılı olarak bilgilendirilmelidir,
3. Olayın tekrarlamaması için Risk Analizi gerçekleştirilerek uygun kontroller tanımlanmalıdır.

J. AĞ ÜZERİNDEN SALDIRI:

1. Ağ üzerinden gerçekleşen ve tespit edilen tüm ağ anormallikleri ve saldırılara zaman kaybetmene BGYS yöneticisine iletilmelidir,
2. Saldırıya SOME PROSEDÜRÜ çerçevesinde zaman kaybedilmeden reaksiyon gösterilmelidir,
3. Olay ile ilgili yasal takibat gereken bir durum olmasından dolayı yetkili kişiler/makamlar Üst yönetimin onayı ile yazılı olarak bilgilendirilmelidir,
4. Olayın tekrarlamaması için Risk Analizi gerçekleştirilerek uygun kontroller tanımlanmalıdır.

K. YANGIN, DEPREM, SU BASKINI GİBİ OLAĞAN ÜSTÜ HALLER:

1. İlgili olağan üstü hal zaman geçirilmeden BGYS yöneticisine ve iletişim kısmında tanımlanmış olan birimlere, sırasıyla ve zaman geçirilmeden bildirilmelidir,
2. Yangın ve sel durumunda can güvenliğini tehlikeye atmayacak şekilde Önemlilik sırasına göre evrak, sistem ve diskler kurtarılmalıdır,
3. Olay ile ilgili yasal takibat gereken bir durum olmasından dolayı yetkili kişiler/makamlar Üst yönetimin onayı ile yazılı olarak bilgilendirilmelidir,
4. Olayın tekrarlamaması için Risk Analizi gerçekleştirilerek uygun kontroller tanımlanmalıdır.

L. ENERJİ, İKLİMLENDİRME, VB. HİZMET KESİNTİLERİ:

1. Elektrik kesintilerinde zaman kaybedilmeden ilgili sistem yöneticisine ve BGYS yöneticisine durum bildirilmelidir,
2. Hissedilir voltaj dalgalanmalarında BGYS yöneticisine bildirilmelidir,
3. Voltaj seviyesini gerçek zamanlı takibini sağlayan donanımlar bulundurulmalıdır,
4. Enerji kesintisi meydana geldiğinde sistemlerin ani kapanmasının önlenmesi için kademeli ve kontrollü şekilde sistemler kapatılmalıdır,
5. Enerji kesintisi hizmet veren firmaya/kuruma yukarıda tanımlanan iletişim kanallarından bildirilmelidir,
6. KGK (UPS), vb. devreye girdiği ve yükleri besleyebileceği güç değeri takip edilmelidir,
7. Jeneratörün devreye girip girmediği kontrol edilmelidir,
8. Klima, vb. iklimlendirme sistemi arızalarında zaman kaybedilmeden Sistem odası sorumlusuna ve BGYS Yöneticisine bildirilmelidir,
9. Olay ile ilgili yasal takibat gereken bir durum olması durumunda yetkili kişiler/makamlar Üst yönetimin onayı ile yazılı olarak bilgilendirilmelidir,

10. Olayın tekrarlamaması için Risk Analizi gerçekleştirilerek uygun kontroller tanımlanmalıdır.

M. İNTERNET SERVİS SAĞLAYICI (ISS) KAYNAKLI ARIZA ve KESİNTİLER:

1. İnternet bağlantısında sorun ile karşılaşıldığında Ağ Yöneticisine bildirilmelidir,
2. İnternet bağlantısı ile ilgili sorun yaşandığında, DNS sunucularından kaynaklı kesinti olup olmadığı ping (8.8.8.8, vb.) komutu ile genel ve açık sistemlere gönderilen paketler ile sorgulanmalı,
3. Şayet dış ağa erişilemiyorsa iç ağ geçidine ping testi gerçekleştirilir, yönlendiriciye erişiliyorsa, ilgili modem/router (ADSL, G.SHDSL, Fiber…) ile servis sağlayıcı arasındaki bağlantı kontrolü yapılmalı ve Servis Sağlayıcı ile yukarıdaki iletişim bilgileri aracılığı ile bağlantıya geçilmelidir,
4. Olayın tekrarlamaması için risk analizi gerçekleştirilerek uygun kontroller tanımlanmalıdır.

N. TANIMLI OLMAYAN DİĞER BİLGİ GÜVENLİĞİ OLAYLARI:

1. Yukarıda belirtilen olay tanımlarına uymayan ancak Bilgi varlıklarının Gizlilik, Bütünlük ve Erişilebilirliğine zarar verebilecek olaylar BGYS Yöneticisine bildirilmelidir,
2. Tanımlanmayan olay sınıflandırılarak bu Prosedüre girilmelidir,
3. Olay ile ilgili yasal takibat gereken bir durum olmasından dolayı yetkili kişiler/makamlar Üst yönetimin onayı ile yazılı olarak bilgilendirilmelidir,
4. Olayın tekrarlamaması için Risk Analizi gerçekleştirilerek uygun kontroller tanımlanmalıdır.

İLGİLİ REFERANS DOKÜMANLAR VE KONTROL MADDELERİ:

REFERANS VERİLEN:

REFERANS ALINAN:

1. A.11.1.2
2. A.11.1.3
3. A.11.1.4
4. A.12.1.1
5. A.16.1.1
6. A.16.1.2
7. A.16.1.3
8. A.16.1.4
9. A.16.1.5
10. A.16.1.6
11. A.16.1.7

Bu sayfa son olarak 05 Aralık 2021 tarihinde ve 14.41 saatinde düzenlenmiştir.