#### EK-06 RİSK HESAPLAMA FAKTÖRLERİ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **VARLIK DEĞERİ TABLOSU** | | | | |
| **GÜVENLİK**  **HEDEFİ** | **DÜŞÜK (1)** | **ORTA (2)** | **YÜKSEK (3)** | **ÇOK YÜKSEK (4)** |
| **GİZLİLİK** | Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz.  Açığa çıkan hassas olmayan bilgileri kurumu etkilemez / çok az etkiler. | Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz. Açığa çıkan kritik bilgi kurumu etkiler. Söz konusu bilgi sadece kurum içerisindeki personelin bilmesi gereken bilgidir. Etki orta vadede telafi edilebilir. | Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkar. Açığa çıkan kritik bilgi kurumu etkiler. Etki orta vadede telafi edilebilir. Söz konusu bilgi kuruma ve kişiye ait gizli bilgilerdir. (program, uygulama yazılımları, EBYS, ÇKYS vb, bilgisayar şifre ve /veya parolaları, kişisel bilgiler,  sözleşme bilgileri, ihale bilgileri, personel bilgileri, hasta bilgileri) | Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkar. Açığa çıkan kritik bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir. (Kuruma ait çok gizli bilgiler -sistem, sunucular, network cihazları, veri tabanları erişimleri sağlayan şifre ve /veya parolalar, kurum stratejileri vb.- yetkisiz kişilerin eline geçmesi durumunda Sağlık Bakanlığına büyük ölçüde zarar verecek her türlü bilgi.) |
| **BÜTÜNLÜK** | Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen hassas olmayan bilgiler kurumu  etkilemez / çok az etkiler. | Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen kritik bilgi kurumu etkiler. Etki orta vadede telafi edilebilir. (Elektronik imza /  kayıt onay mekanizmasının kullanıldığı bilgi varlıkları) | Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişir. Kontrol dışı değişen kritik bilgi kurumu etkiler. Etki orta vadede telafi edilebilir. (Her kayıt için onay sürecinin olduğu,  değişiklik kayıtlarının tutulduğu bilgi varlıkları) | Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişir. Kontrol dışı değişen kritik bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir. (Zaman damgalı elektronik imzanın kullanıldığı, onay kayıt sürecinin her adımda işlendiği bilgi varlıkları) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **VARLIK DEĞERİ TABLOSU** | | | | |
| **GÜVENLİK**  **HEDEFİ** | **DÜŞÜK (1)** | **ORTA (2)** | **YÜKSEK (3)** | **ÇOK YÜKSEK (4)** |
| **ERİŞİLEBİLİRLİK / KULLANILABİLİRLİK** | Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen hassas olmayan bilgiler kurumu etkilemez / çok az etkiler. (Uzun süreli kesintilerde iç ve dış hizmetleri aksatmayan bilgi varlıkları.) | Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen kritik bilgi kurumu etkiler. Etki orta vadede telafi edilebilir. (Kurumda verilen hizmetlerde her hangi bir kesinti/aksama durumunda tolere edilebilecek süre 3 saat olup, bu süre içinde erişilebilir  hale getirilmesi gereken bilgi varlıkları-AD, Exchange vb.) | Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilemez. Erişilebilirliğine zarar gelen bilgi kurumu etkiler. Etki orta vadede telafi edilebilir. (Kurumda verilen hizmetlerde her hangi bir kesinti/aksama durumunda tolere edilebilecek süre 1 saat olup, bu süre içinde erişilebilir hale getirilmesi gereken  bilgi varlıkları -IIS-Uygulama sunucuları – veritabanı - FW) | Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilemez. Erişilebilirliğine zarar gelen bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir. Kurumda verilen hizmetlerde her hangi bir kesinti/aksamaya tahammül bulunmamaktadır. |
| 1. Tanımlanan her bir varlık için, varlık sahibi tarafından değer atanmalıdır. 2. Bir varlığın değerini belirlemek için Genel Müdürlüğümüz tarafından oluşturulan temel referans; varlığın gizlilik, bütünlük ve/veya erişilebilirliğini yitirdiğinde oluşabilecek zarardır. Yerine koyma maliyeti, gizli bilginin ifşası neticesinde oluşabilecek kurumsal itibar gibi soyut kavramlar da göz önüne alınmalıdır. 3. Varlık sorumlusu, varlığa değer belirleme aşamasında gizlilik, bütünlük ve erişilebilirlik için ayrı değerler atayabilir. Örneğin bir web sitesi için değer atanırken;   \*web sitesinin gizlilik değeri için düşük - 1 puan (açığa çıkan bilgi kuruma zarar vermez),  \*web sitesinin erişilebilirlik değeri için orta - 2 puan (3 saate kadar ulaşılamaması durumunda hizmet süreci aksamaz)  \*web sitesinin bütünlük değeri için yüksek - 3 puan (kontrol dışı değişen bilgi kuruma zarar verir) atayabilir.  Bu durumda varlığa verilecek nihai değer, belirlenen tüm değerlerin maksimumu olmalıdır.  Varlık sahibi tarafından varlığa atanan değer, varlığın korunması için harcanacak kaynakların belirlenmesi için referans değer oluşturacağı için dikkatlice değerlendirilerek atanması gerekir. | | | | |

|  |  |
| --- | --- |
| **RİSKİN GERÇEKLEŞME OLASILIĞI** | |
| **Düşük (1)** | Bilgi Güvenliği İhlali, saldırı, olumsuz bir olayın olma ihtimali  %1 ile %10 arasındadır. |
| **Düşük (2)** | Bilgi Güvenliği İhlali, saldırı, olumsuz bir olayın olma ihtimali 11% ile %39 arasındadır. |
| **Orta (3)** | Bilgi Güvenliği İhlali, saldırı, olumsuz bir olayın olma ihtimali 40% ile %69 arasındadır. |
| **Yüksek (4)** | Bilgi Güvenliği İhlali, saldırı, olumsuz bir olayın olma ihtimali 70% ile %80 arasındadır. |
| **Çok Yüksek (5)** | Bilgi Güvenliği İhlali, saldırı, olumsuz bir olayın olma ihtimali en az 81% ve üzeridir. |

|  |  |
| --- | --- |
| **GİZLİLİK ETKİ DEĞERİ** | |
| **Düşük (1/2)** | Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliği olayının sonucunda riskin gizliliğe etkisi düşük olur. Kurum imajı etkilenmez, zarar çok kısa vadede telafi edilebilir ve iş süreci aksamaz. |
| **Orta (3)** | Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliği olayının sonucunda riskin gizliliğe etkisi orta derecede olur. Kurum imajı belirli oranda zarar görür. İtibar kaybı ve yasal yükümlülük açısından zarara yol açmaz. |
| **Yüksek (4)** | Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliği olayının sonucunda riskin gizliliğe etkisi yüksek şiddette olur. Medyada yayınlanacak şekilde kurum imajı zedelenir. Zarar orta vadede telafi olunur. Yüksek ek maliyetler doğar ya da çalışanların motivasyonu üzerinde ciddi olumsuz etkiye yol açar. |
| **Çok Yüksek (5)** | Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliği olayının sonucunda riskin gizliliğe etkisi çok yüksek şiddette olur. Yıkıcı / felaket düzeyinde etki gerçekleşir. Kurum çok ciddi itibar kaybına uğrar. Yasal yükümlülükler doğurur ve çok yüksek ek maliyetler doğar. |

|  |  |
| --- | --- |
| **BÜTÜNLÜK ETKİ DEĞERİ** | |
| **Düşük (1/2)** | Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliği olayının sonucunda riskin bütünlüğe etkisi düşük olur. Bütünlük ihlali kurum imajını etkilemez. Sistem ve işleyişte performans sorunu gerçekleşmez. |
| **Orta (3)** | Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliği olayının sonucunda riskin bütünlüğe etkisi orta derecede olur. Bütünlüğü kaybedilen bilgi kurum imajına zarar verir. Ek iş maliyetlerinin doğmasına neden olur. |
| **Yüksek (4)** | Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliği olayının sonucunda riskin bütünlüğe etkisi yüksek şiddette olur. Kritik iş süreçlerinin zarar görmesi kuruma kritik derecede zarar verir. |
| **Çok Yüksek (5)** | Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliği olayının sonucunda riskin bütünlüğe etkisi çok yüksek şiddette olur. Bütünlüğün sağlanamaması felaket düzeyde etkiye neden olur. Yasal yükümlülükler doğurur, çok yüksek ek maliyetler doğar. |

|  |  |
| --- | --- |
| **ERİŞİLEBİLİRLİK ETKİ DEĞERİ** | |
| **Düşük (1/2)** | Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliği olayının sonucunda riskin erişilebilirliğe etkisi düşük olur. Risk kurum dışına yansıyacak düzeyde değildir. İş süreçlerinin aksamasına neden olmaz. |
| **Orta (3)** | Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliği olayının sonucunda riskin erişilebilirliğe etkisi orta derecede olur. Belirli bir hizmette yavaşlama ya da küçük çapta iş kesintileri oluşur. Erişilemeyen bilgi orta vadede yerine  koyulabilir. |
| **Yüksek (4)** | Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliği olayının sonucunda riskin erişilebilirliğe etkisi yüksek şiddette olur. Olumsuzluk kurum dışına yansır. İş kaybı oluşur, yüksek  maliyetler doğar. |
| **Çok Yüksek (5)** | Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliği olayının sonucunda riskin erişilebilirliğe etkisi çok yüksek şiddette olur. Kurum çok ciddi iş kaybına uğrar. Etki yıkıcı / felaket düzeyinde olur. Yasal yükümlülükler doğar. Zarar telafi edilemez / uzun vadede telafi edilebilir. |