|  |  |  |  |
| --- | --- | --- | --- |
| 1.İhlal Olayı Tarihi |  | 3.İlişkili Olay/İhlal Olayı Numaraları |  |
| 2. İhlal Olayı No |  |  |
| **4.İLETİŞİM NOKTASI OLAN KİŞİ** | | | |
| 4.1.Ad-Soyad |  | 4.3.Bölüm |  |
| 4.2.Telefon |  | 4.4.E-Posta |  |
| **5.BG İHLAL OLAYLARINA MÜDAHALE EKİBİ ÜYESİ** | | | |
| 5.1.Ad-Soyad |  | 5.3.Bölüm |  |
| 5.2.Telefon |  | 5.4.E-Posta |  |
| **6.BİLGİ GÜVENLİĞİ İHLAL OLAYININ TANIMI** | | | |
| 5.1.Ne Oldu? |  | | |
| 5.2.Nasıl Oldu? |  | | |
| 5.3.Neden Oldu? |  | | |
| 5.4.Etkilenen Varlıklara Dair İlk İzlenimler |  | | |
| 5.5.Kurumun Ticari Faaliyetine Etkileri |  | | |
| 5.6.Tespit Edilen Teknik Açıklık |  | | |
| **7.BİLGİ GÜVENLİĞİ İHLAL OLAYININ DETAYLARI** | | | |
| 7.1.İhlalin Meydana Geldiği Tarih-Saat | |  | |
| 7.2.İhlalin Tespit Edildiği Tarih-Saat | |  | |
| 7.3.İhlalin Raporlandığı Tarih-Saat | |  | |
| 7.4.İhlale Müdahale Tamamlandı mı? | | EVET  HAYIR | |
| 7.5.İhlalin Durdurulma Süresi (Gün/Saat/Dakika) | |  | |
| 7.6 Yanlış Alarm | | EVET  HAYIR | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **8.bilgi güvenliği ihlali kategorisi** | | | | | | |
| Sadece bir tanesi seçilebilir: | | | | | | |
| 8.1 KESİN (İhlal Oluştu) | | | | 8.2 ŞÜPHELİ (İhlal Kesinleşmedi) | | |
| **9.İHLAL kategorisi**  Aşağıdakilerden uygun olanı seçiniz | | | | | | |
| **9.1 UTİLİTE HİZMETLERİNİN DURMASI** | | | | | | |
| Enerji Kesilmesi | Klima Sisteminin Durması | | | İletişim Araçlarının  Arıza Yapması | | |
| **9.2 TEKNİK** | | | | | | |
| Ekipman Arızası | Ekipmanın Hatalı Çalışması | | | | Yazılımın Hatalı Çalışması | |
| Bilgi Sistemlerinin Sürdürülebilirliğinin Bozulması | | | | Kapasite Yetersizliği | | |
| **9.3 YETKİSİZ UYGULAMALAR** | | | | | | |
| Yetkisiz Ekipman Kullanımı | | | | Veri Yolsuzluğu | | |
| Verinin Yasal Olmayan Şekilde Proseslenmesi | | | | Sahte Veya Kopya Yazılım Kullanma | | |
| Yazılımın Hileli Yoldan Kopyalanması | | | |  | | |
| **9.4 IT/IK PERSONELİ** | | | | | | |
| Hatalı Kullanım | Yetkinin Suistimali | | | Haklarin Amacı Dışında Kullanımı | | |
| Yapılan İşlemin İnkar Edilmesi | | | | Yetkili Kişiye Ulaşılamaması | | |
| **9.5 İNSAN KAYNAKLI İHLALLER** | | | | | | |
| Endüstri Casusluğu | | Eğitimsiz Çalışan | | | | |
| Computer Criminal | | Terörist | | | | |
| Hacker/Cracker | | | | | | |
| Computer criminal, terrorist, hacker/cracker ihlallerinde alttakilerden uygun olan seçeneği de -tespit edildiyse- işaretleyiniz: | | | | | | |
| Zararlı Yazılım (Solucan, Truva Atı, Virüs vs.) | | | | Oltalama | | DoS/DDoS |
| Man In the Middle | SQL Injection | | | Cryptojacking | | |
| Zeroday Exploit | Parola Saldırısı | | | Eavesdropping Attack | | |
| Doğumgünü Saldırısı | Diğer  Tanımlayınız: | | | | | |
| **9.6 SİYASİ/TOPLUMSAL** | | | **9.7 DİĞER** | | | |
| Erişimin Engellenmesi | | | Tanımlayınız: | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **10.ETKİLENEN BİLGİ VARLIKLARI** | | | | | | |
| **10.1 eTKİLENEN BİRİNCİL VARLIKLAR** | | | | | | |
|  | | | | | | |
| **10.2 etkilenen ikincil varlıklar** | | | | | | |
|  | | | | | | |
| **11.İŞE OLUMSUZ ETKİSİ** | | | | | | |
|  | | | | | | |
|  | |  | İhlalin işe etkisi (1-5) | | | |
| 11.1 Gizlilik | |  |  | | | |
| 11.2 bütünlük | |  |  | | | |
| 11.3 erişilebilirlik | |  |  | | | |
| 11.4 operasyon | |  |  | | | |
| **12. ihlalden kurtarma maliyeti** | | | | | | |
| İhlalden sistemi geri kurtarmak için alınan aksiyonlar bütçeli çalışmalar ise bunlara ait maliyetleri kaydedin | | | | | | |
| **kurtarma aksiyonu** | | | | | | **maliyeti** |
|  | | | | | |  |
|  | | | | | |  |
|  | | | | | |  |
|  | | | | | |  |
|  | | | | | |  |
|  | | | | | |  |
| **toplam:** | | | | | |  |
| **13.ihlalin çözümlenmesi** | | | | | | |
| 13.1 İhlal İnceleme Başlama Tarihi ve Saati | | | |  | | |
| 13.1 İncelemeyi Yapan Kişi(ler) Ad-Soyad | | | |  | | |
| 13.3 İhlalin Sona Erme Tarihi ve Saati | | | |  | | |
| 13.4 İhlalin Etkisini Sona Erme Tarihi | | | |  | | |
| 13.5 İhlal İnceleme Bitiş Tarihi ve Saati | | | |  | | |
| 13.6 İhlal İnceleme Raporunun Referansı ve Yeri | | | |  | | |
| **14.(İHLAL İNSAN KAYNAKLI İSE) İHLALE KATILAN KİŞİLER** | | | | | | |
| Bireysel | | | | Yasal Olarak Yerleşik Kuruluş/Kurum | | |
| Organize Grup | | | | Kaza | | |
|  | | | | Fail Yok | | |
| **15.ihlal olayının FAİLİNİn TANIMI** | | | | | | |
|  | | | | | | |
| **16.GERÇEK YA DA ALGILANAN MOTİVASYON** | | | | | | |
| Cezai/Finansal Kazanç | | | | Eğlence/Hacking | | |
| Siyasal/Terör | | | | İntikam | | |
| Diğer (Belirtiniz) | | | |  | | |
| **17.ihlalE karşılık alınan aksiyonlar** | | | | | | |
|  | | | | | | |
| **18. ihlalE karşılık planlanan aksiyonlar** | | | | | | |
|  | | | | | | |
| **19.bekleyen aksiyonlar** | | | | | | |
|  | | | | | | |
| **20.sonuç** | | | | | |
| İhlal olayının büyüklüğünü belirlemek için “BG İhlal Kategorileri” dökümanından “Sonuç Kriterleri” ni kontrol edin ve uygun olan seçeneği işaretleyin. | | büyük | | küçük | |
| **21.dahili olarak bilgilendirilen kişiler** | | | | | |
| İhlal Olayı yönetimi sürecinde kurum içinde bilgilendirilen kişileri işaretleyiniz: | | Bilgi Güvenliği Yöneticisi | | Bilgi Güvenliği İhlal Olayları Ekibi Yöneticisi | |
| Bilgi Sistemleri Yöneticisi | | İdari Yönetim Yöneticisi | |
| Olayı Raporlayan Kişi | | Olayı Raporlayan Kişinin Yöneticisi | |
| İnsan Kaynaklari | | İcra Kurulu | |
| Diğer  Belirtiniz: | |  | |
| **22.harici olarak bilgilendirilen kişiler/kurumlar** | | | | | |
| İhlal Olayı yönetimi sürecinde kurum dışından bilgilendirilen kişileri/kurumları işaretleyiniz: | | Kolluk Kuvveti | | VERBİS | |
| Müvekkil | |  | |
| Diğer  Belirtiniz: | |  | |
| **23.imzalar** | | | | | |
| raporU HAZIRLAYAN | | KONTROL EDEN | | KONTROL EDEN | |
| İmza: | | İmza: | | İmza: | |
| Ad-Soyad: | | Ad-Soyad: | | Ad-Soyad: | |
| Ünvan: | | Ünvan: | | Ünvan: | |
| Tarih: | | Tarih: | | Tarih: | |
|  | |  | |  | |
|  | |  | |  | |