UYAP Bilgi Güvenliği

Bilgi güvenliği önemli bir konudur. Zira kullanıcı bilgilerinin 3. kişilerle paylaşılması durumunda;

- Veriler çalınabilir, değiştirilebilir, silinebilir ya da çok gizli belgeler görüntülenebilir.
- Çalışılan birimle ilgili bilgiler İnternet'ten yayınlanabilir.
  e-Posta/Haberci hesabı üzerinden kişi adına iletiler gönderilebilir.
  İnteraktif bankacılık hesabındaki paralar çalınabilir.
- Bilgisayarınız üzerinden hesap sahibi adına bilişim suçları işlenebilir.

Bilgi güvenliği, kişiye ait olan bilginin başkasının eline geçmemesini sağlamaktır. Bilginin güvenliği *"gizlilik", "bütünlük"* ve *"erişilebilirlik"* olarak isimlendirilen üç ana unsurdan oluşmaktadır. Bu *3 ana unsurdan* herhangi biri zarar görürse *güvenlik zafiyeti* oluşur.

Gizlilik: Bilginin yetkisiz kişilerin eline geçmemesidir.

Bütünlük: Bilginin yetkisiz kişiler tarafından değiştirilmemesidir.

Erişilebilirlik: Bilginin ilgili ya da yetkili kişilerce ulaşılabilir ve kullanılabilir durumda olmasıdır.

Bilgi Güvenliği Genel Olarak UYAP'ta Nasıl Sağlanmaktadır?

Bilgi Güvenliği Şubesi

Başka hiçbir kamu kurumunda olmayan bir birimdir. Dışarıdan veya içeriden gelebilecek siber tehditlerin önlenebilmesini sağlamak amacıyla UYAP Bilişim Sistemi açıklarını araştırmak ve kapatılmasını sağlamaktan sorumludur.

UYAP Bilgi Sistemi Merkezi Yapıdadır

UYAP Bilgi Sistemi merkezi yapıda çalışmaktadır. Bu şekilde tüm güvenlik çözümleri tek bir merkez üzerinde odaklanmıştır.

Fiziki Güvenlik

UYAP Bilgi Sistemi kendisine ait müstakil bir binada hizmet vermektedir. Bina özel güvenlik alanı olarak ilan edilmiş ve 7/24 güvenlik elemanlarınca korunmaktadır.

Yazılımsal Güvenlik

UYAP Bilgi Sistemleri içerisinde iç ve dış tehditlere karşı dünyaca kabul görmüş "Bilişim Güvenliği Teknolojileri" ile korunmaktadır.

Her bir sistem kendisi içerisinde ayrıca daha önce belirlenen güvenlik politikalarına uygun olarak konfigüre edilmiştir.

N katmanlı Erişim Yapılmaktadır

UYAP Bilgi Sistemlerinde N katmanlı yetkilendirme yapılmaktadır. Yetkilendirme işlemi kullanıcıların kullandıkları bilgisayarlardan başlayarak UYAP içerisinde erişim yapılan dosyalara kadar uzanmaktadır. UYAP Bilgi Sistemi içerisinde bulunan bilgisayarlar ve kullanıcılar Aktif Dizin içerisinde tanımlanmıştır.

UYAP yazılımı içerisinde dosya bazlı yetkilendirme yapılmaktadır. Uygulama Yazılımı da kendi içinde yetki temelli olarak çalışmaktadır. Üstelik yetki unvan, birim ve yer bazında belirlenebilir. Örneğin Uygulama Yazılımı bir zabıt kâtibinin kullanıcı adı ve şifresi ile çalıştırıldığında kullanıcı sadece o zabıt kâtibinin görevli olduğu yerdeki, görevli olduğu mahkemede bulunan dosyaları görebilir ve sadece bu dosyalarda bir zabıt kâtibinin gerçekleştirebileceği işlemleri yapabilir. (Özel önemi olan yetkileri Bilgi İşlem Dairesi Başkanlığı değil ilgili birim verir. Örneğin teftiş yetkisini Teftiş Kurulu Başkanlığı, gizli sicil görme yetkisini Personel Genel Müdürlüğü verir gibi.)

Yapılan işlemler loglanmaktadır. UYAP Bilgi Sistemini kullanan kullanıcıların sistem üzerindeki tüm hareketleri loglanmaktadır. Kullanıcı Adı, Bilgisayar Adı, Mac Adresi, IP numarası, Tarih-Saat, Ekran, Değişiklik, Evrak Görüntüleme dâhil kayıt altına alınmaktadır.

UYAP İç Güvenlik Sistemi

- UYAP Bilgi Sisteminde "Loglama" mekanizması kurulmuştur.
- Windows İşletim Sistemi kullanılmıştır.
- Son kullanıcılar üzerinde güvenlik önlemleri alınmıştır.

UYAP Dış Güvenlik Sistemi

UYAP sistemi dış tehditlere karşı üstünlüğü ve etkinliği dünyaca kabul görmüş "Bilişim Güvenliği Teknolojileri" ile korunmaktadır. Dış güvenlik kapsamında aşağıdaki güvenlik tedbirleri mevcuttur:

- İntranet: UYAP kendi iç network (İnternet ağı) içinde çalışmaktadır.
- Noktadan Noktaya VPN (Virtual Private Network): Taşra birimleri UYAP'a İnternet üzerinden erişir ama bu erişimi kendileri için özel olarak oluşturulmuş bir tünel içinden geçerek yaptıkları için talep ettikleri veya gönderdikleri bilgileri diğer İnternet kullanıcıları göremez.
- Firewall: İletişim trafiği Güvenlik Duvarları kontrolündedir. Tanımlanan kurallar basit ve etkilidir: "A, B, C trafiğine izin ver, bunlar dışındakilerin hepsini yasakla!"
- IDS (Saldırı Tespit Sistemi) ve IPS (Saldırı Önleme Sistemi) modüllerine sahiptir.
- NAT (Network Address Translation): Kullanıcı ve sunucuların gerçek IP'leri dışarıdan görülmüyor.
- Proxy (İçerik Denetimi): Kullanıcıların erişimi tek bir İnternet çıkışı üzerinden olduğu için kontrolü ve denetimi kolay ve ayrıca güvenlidir.
- Merkezde ve Kullanıcılarda Anti virüs
- Merkezde Saldırı Önleme Sistemi

- En yeni teknoloji Swich, Router vs. donanımlar
- Sayısal İmza
- Acil Durum Merkezi

UYAP Bilgi Güvenliği Yönetim Sistemi (BGYS)

Vazgeçilmez ve önemli bilgi sistemlerinin korunabilmesi, iş risklerinin en aza indirgenmesi ve iş sürekliliğinin sağlanması ancak bütünsel yaklaşımlar ile mümkündür. Tüm bunlardan çıkan sonuç bilgi güvenliğinin bir teknoloji sorunu olmadığı, bunun bir iş yönetimi sorunu olduğudur.

İşte bu nedenlerle "Kurumsal Bilgi Güvenliği" kavramı altında bir yönetim sistemi oluşturma yönünde yapılan çalışmalar 1993 yılında BS 7799 standardını, 2000 yılında ISO/IEC 17799 standardını ve 2006 yılında ISO/IEC 27001 standardını ortaya çıkarmıştır. Kısaca ISMS (Information Security Management System)/BGYS (Bilgi Güvenliği Yönetim Sistemi) olarak adlandırılan bu yeni yönetim sistemi standardı "bilgilerin" her türlü ortamda (kâğıt üzerinde, elektronik ortamda, yazılı ve sözlü iletişimde vb.) güvenliğini sağlamak için öngörülen yönetsel çerçeveleri oluşturur ve bilgi güvenliğini kurumsal süreçlerin bir parçası (iş anlayışı, yönetim ve kültür sorunu) hâline getirir.

Yardım Masası

Adalet Bakanlığı personelinin, kişisel olarak kullanımı için düzenlenmiş portal hesabı bulunmaktadır ve Yardım Masasına ulaşmak için portal giriş şifresini yazdıktan sonra gelen ekranda dikey olarak düzenlenmiş bulunan butonlar bulunmaktadır. Bu butonlar sıra ile UYAP uygulamaları, UYAP1 uygulamaları ve Yardım Masası şekliyle düzenlenmiştir. Bu ekranda bulunan Yardım Masası tıklandığı zaman açılan ekranda Ana sayfa, Olay İzleme, Yeni Olay Talebi, Çözüm Bul ve Kullanım Butonları bulunur. İletilmek istenen bir konu varsa bunu Yeni Olay Talebi butonunu tıklayarak yapmak mümkündür.

UYAP yaygınlaştırma çalışmalarının sonuna gelinmesi ile birlikte Yardım Masası faaliyetlerinin taşra birimlerinde görevlendirilen uzman kullanıcılar yardımıyla yürütülmesi amacıyla taşra yardım masası birimlerinin kurulması ve bakanlık yardım masasının şubesi olarak görev yapmasının sağlanması.

Spectra programının taşrada görevlendirilmiş bulunan uzman kullanıcıların da kullanımına açılması için gerekli altyapı ve program güncelleştirilmesinin yapılması.

Kullanıcıların yardım masasını daha etkin kullanımının sağlanmasıdır.

Ulusal Yargı Ağının Adalet Bakanlığına bağlı tüm birimlerde yaygınlaşmasıyla birlikte meydana gelen sorunlarda kullanıcının her zaman yanında olmak,

Kullanıcının karşılaştığı ve tek başına çözemediği durumlarda her zaman arayacağı bir pozisyonda bulunmak.

Sistemdeki tüm kullanıcıların (e-Posta sorunu, şifre verme/silme/değiştirme/.) teknik sorunlarını çözmek.

Gelen bu talepler değerlendirilerek kullanıcıya ulaşma imkânı varsa telefonla bilgi vermek gerekli ise Türk Telekom (Avea) kurumsal hattı bulunan yerler aranarak konu hakkında açıklayıcı bilgi verilir, eğer Türk Telekom (Avea) hatlı telefon bildirilmemişse, gelen talebe uygun olarak üretilen çözüm yine Spectra üzerinden kullanıcıya iletmek.

Telefonla gelen çağrıları karşılamak, arayan kişilere sistemle ilgili bilgilendirme yapmak.

UYAP sistemine yönelik olarak gelen öneri ve istekler yine ilgili Uygulama ve Geliştirme Şubesi personeline aktarmak.

Yardım Masasına telefonla gelen uygulama ile ilgili taleplerde kullanıcıya gerekli bilgiyi vermek ve sorunu en kısa sürede çözmek. Bunun yanında bundan sonraki sorunlarının çözümü için yardım masasını kullanması ve buradan talebini takip etmesi hususunda bilgi vermektir.