UYAP BİLGİ GÜVENLİĞİ

1. *UYAP'ta ve tüm dünyada bilgi güvenliği konusunda hangi kavramlar öne çıkmıştır?*
Cevap:

- Gizlilik (confidentiality)
- Bütünlük (integrity)
- Erişilebilirlik (availability)

2. *UYAP'ın sistem güvenliği özellikleri nelerdir?*
Cevap:

- Teşhis ve Doğrulama
- Kayıt Edilebilirlik
- Verilerin Bütünlüğü
- Açık Anahtar Altyapısı ve Elektronik İmza Servisleri
- Emniyetli Mesaj ve Doküman Servisi
- Ağ Güvenliği
- Uzaktan Erişim Güvenlik Servisi

3. *UYAP'ın sistem güvenliği özelliklerinden biri olan "Teşhis ve Doğrulamayı" gizlilik, bütünlük ve erişilebilirlik kavramlarıyla birlikte açıklayınız?*
Cevap: Sistem, UYAP sistemine bağlanan her kullanıcıyı teşhis ederek kullanıcı bazında kayıt tutabilme yeteneğine sahiptir. Bunun için her kullanıcının herhangi bir işlem yapmadan önce sisteme kendisini tanıtması zorunlu kılınarak kullanıcının kimliği ile kullanıcının kaydını tutabilmekte, bütün işlemlerini birbirine ilişkilendirebilecek kabiliyettedir.

4. *UYAP'ın sistem güvenliği özelliklerinden biri olan "Kayıt Edilebilirliği" gizlilik, bütünlük ve erişilebilirlik kavramlarıyla birlikte açıklayınız?*
Cevap: Sistem, kayıt edilebilir olayların kayıtlarının yaratılmasını, idamesini, analiz edilmesini ve yetkisiz değiştirme, erişim ve silmeye karşı korunmasını sağlayacak kabiliyettedir. Denetim kayıtları ve diğer bilgiler arasında ayrım sağlamakta, denetim kaydı verilerine sadece sistem yöneticisinin erişebilmesini sağlamakta ve izinsiz erişimlerden korumaktadır. Kayıt işlemlerinin ve denetim kaydı verisinin normal kullanıcılar tarafından değiştirilebilmesini ve silinmesini engellemekte, seçilen bir veya birden fazla kişinin eylemleri ile ilgili kayıtların kişi bazında tutulmasını sağlamaktadır.

5. *UYAP'ın sistem güvenliği özelliklerinden biri olan "Verilerin Bütünlüğünü" gizlilik, bütünlük ve erişilebilirlik kavramlarıyla birlikte açıklayınız?*
Cevap: Sistem, **sayısal imza** ve mesaj özeti mekanizmalarını kullanarak kritik bilgilerin izinsiz değiştirildiği ve silindiği zaman bunu tespit etmekte, virüs gibi izinsiz olarak sistemdeki verileri değiştirip, silinebilen zararlı kodları tespit edip yok edecek kabiliyette tasarlanmıştır.

6. *UYAP'ın sistem güvenliği özelliklerinden biri olan "Açık Anahtar Altyapısı ve Elektronik imza Servislerini" gizlilik, bütünlük ve erişilebilirlik kavramlarıyla birlikte açıklayınız?*
Cevap: Sistem, sayısal imza ve kimlik doğrulama servislerini desteklemek üzere kurulmuş olan Açık Anahtar Altyapısı (örneğin; kullanıcı anahtarlarının ve sertifikalarının yaratılması, güncellenmesi, iptal edilmesi) için sertifikasyon yetkilisi yazılımı ile Açık Anahtar Altyapısı istemci yazılımlarını kullanmaktadır. Sertifikasyon yetkilisi, kullanıcı anahtar çiftinin ve sertifikalarının yaratılması, güncellenmesi, iptal edilmesini sağlamaktadır. Sertifikasyon yetkilisi kendi gizli anahtarlarını gizli tutmaktadır. Sistemdeki anahtar yönetimi işlevinden de yine sertifikasyon yetkilisi sorumludur. Anahtar yönetimi, sistemdeki her gerekli birim için aşağıda belirtilen işlevleri karşılamaktadır.

- Anahtar yönetimi
- Anahtar dağıtımı
- Anahtar doğrulanması ve anahtar iptal edilmesi
- Anahtar süresinin bitirilmesi
- Anahtar bildirimi
- Anahtar kimlik doğrulaması

Açık anahtar altyapısı istemcisi ise kullanıcı adına sertifikasyon yetkilisi tarafından sağlanan Açık Anahtar Altyapısı servislerini doğrudan kullanarak gerekli işlemlerin yerine getirilmesini sağlamaktadır.

7. *UYAP'ın sistem güvenliği özelliklerinden biri olan "Emniyetli Mesaj ve Doküman Servisini" gizlilik, bütünlük ve erişilebilirlik kavramlarıyla birlikte açıklayınız?*
Cevap: Sistem, belirlenmiş kullanıcılar ve uygulamalar için emniyetli mesaj servisini sağlamakta, belirlenmiş kullanıcılar tarafından gönderilen mesajların veya hazırlanan dokümanların içeriğinin yazılım olarak şifrelenmesini temin etmektedir. Sistem, belirlenmiş kullanıcılar tarafından gönderilen mesajların veya hazırlanan dokümanların sahibinin kimliğinin doğrulanması için sayısal olarak imzalanmasını, mesajın ya da dokümanın sayısal imzanın doğrulanarak mesaj veya doküman sahibinin kim olduğunun teşhisini ve doğruluğunun kanıtlanmasını sağlamaktadır.

8. *UYAP'ın sistem güvenliği özelliklerinden biri olan "Ağ Güvenliğini" gizlilik, bütünlük ve erişilebilirlik kavramlarıyla birlikte açıklayınız?*

Cevap: Sistemin ağ güvenliği, her lokasyonun çıkışında "VPN" ve tüm bağlantıları kontrol eden güvenlik duvarı yazılımı (Firewall) ile sağlanmaktadır.

9. *UYAP'ın sistem güvenliği özelliklerinden biri olan "Uzaktan Erişim Güvenlik Servisini" gizlilik, bütünlük ve erişilebilirlik kavramlarıyla birlikte açıklayınız?*
Cevap: Sisteme, internet gibi güvensiz ortamda herhangi bir noktadan erişildiğinde, iletilen bilgilerin güvenliği için aşağıdaki koşullar sağlanmıştır.

- Sunucu ve kullanıcının birbirlerinin kimliğini doğrulaması,
- Kullanıcının ağ üzerinde bağlantı kurduğu sunucunun DNS adresinin ve isminin sertifikalar yoluyla doğrulanması,
- Sunucu ve istemci arasında kurulan bağlantının kriptolanması, veri bütünlüğünün sağlanması ve anahtarların değiştirilmesi,
- Sunucu ve kullanıcı arasındaki veri alışverişinin güvenliği için SSL (Secure Socket Layer) protokolü kullanılmaktadır.

10. *UYAP'tan başka hiç bir kamu kurumunda olmayan şubenin adı nedir?*
Cevap: UYAP'tan başka hiç bir kamu kurumunda olmayan "Bilgi Güvenliği Şubesi" bulunmaktadır.

11. *"Bilgi Güvenliği Şubesinin" görevlerini açıklayınız?*
Cevap: Bilgi Güvenliği şubesinin görevleri, dışarıdan veya içeriden gelebilecek saldırıları önlemek amacıyla UYAP Bilişim Sisteminin açıklarını araştırmak ve kapatılmasını sağlamaktır.

12. *"Sayısal İmza" nedir, açıklayınız?*
Cevap: İngilizce digital signature kelimesinin Türkçe karşılığı olup, günümüzde yüksek güvenlik gereksinimini karşılamada kullanılan tekniklerden biridir. Özetle, her insanın parmak izi kadar benzersiz olan ancak sanal dünyada kullanılan kimlik belirtecidir.

UYAP İÇ GÜVENLİK SİSTEMİ

13. *UYAP Bilgi Sistemi hangi servisten faydalanarak çalışır, açıklayınız?*
Cevap: Bilgi Sistemi Aktif Dizin Servisinden faydalanarak çalışır.

- Aktif dizin, Windows platformunda çalışan sistemlerde kullanılan servistir. Network üzerindeki nesneler (kullanıcı, kullanıcı grupları, bilgisayarlar, organizasyonel birimler vs.) hakkındaki bilgilerinin kayıtlı olduğu yerdir. Aktif dizine tanıtılmamış kullanıcı, kurumun Bilişim Sisteminden faydalanamaz.
- Bilişim Sisteminde uyulması gereken temel güvenlik kurallarının merkezden belirlenebilmesini sağlamaktadır.
- Merkezden belirlenen temel güvenlik kurallarına bütün kullanıcılar tarafından uyulduğunu garanti etmektedir.

14. *UYAP Bilgi Sisteminin kullanılabilmesi için hangi ön şartların gerçekleşmesi gerekmektedir?*
Cevap: 1990-2000 döneminde sözcük işlemcilerin gelişimine en büyük etki işletmelerde ve evlerde en yaygın kullanılan Intel-Microsoft tabanlı bilgisayarlarda Microsoft Windows grafik arayüzlü işletim sisteminin yaygınlaşmasıyla sağlanmıştır. 1993 yılında piyasaya çıkan Windows 3.1 ile DOS işletim sistemi kullanıcıları pencere kullanımıyla tanışmış, 1995 yılında piyasaya çıkan Windows 95, DOS işletim sisteminin yerini almıştır. Fare ile ekranda görsellerle desteklenmiş standart menüler, bağlam menüleri, düğmeler, açılır listeler, çoklu iletişim pencereleri ve sihirbazların kullanımıyla yazılımlar kolaylaşmıştır. Bu dönemde sözcük işlemciler, işlem tablosu ve sunum hazırlama yazılımlarıyla bir paket haline getirilerek ofis takımları hâlinde pazarlanmaya başlamışlardır.

- Kullanıcı olabilmek için Personel Genel Müdürlüğü kayıtlarında bulunmak gerekmektedir.
- Sisteme giriş için bir "kullanıcı adı" ve "parola" ya ihtiyaç vardır. Parola Bilgi İşlem Dairesi Başkanlığı tarafından verilir. Kullanıcı tarafından sonradan değiştirilebilir.
- Uygulama Yazılımının çalıştırabilmesi için de ayrıca bir parolaya sahip olunması gerekir. Bu parola da Bilgi İşlem Dairesi Başkanlığı tarafından verilir ve ilk kullanımında kullanıcı tarafından değiştirilmesi zorunluluğu vardır.
- 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 gibi)

15. *UYAP Bilgi Sisteminde hangi mekanizma kurulmuştur, açıklayınız?*
Cevap: UYAP Bilgi Sisteminde "Loglama" mekanizması kurulmuştur. UYAP bilgi sistemini kullanan kullanıcıların sistem üzerindeki hareketleri Kullanıcı Adı, Bilgisayar Adı, Mac Adresi, IP numarası, Tarih-Saat, Ekran, Değişiklik bazında kayıt altına alınmaktadır.

16. *UYAP Bilgi sisteminde hangi işletim sistemi kullanılmıştır ve kullanılma nedenlerini açıklayınız?*
Cevap: Windows işletim sistemi kullanılmıştır. Bu sayede,

- Bilgisayarlar merkezi olarak yönetilebilmekte,
- UYAP uygulaması için gerekli olan JAR dosyalarının merkezi dağıtımı yapılabilmekte,
- Kimlik doğrulama işlemi yapılabilmekte,
- Son kullanıcı bilgisayarında kullanıcı bazlı yetkilendirmesi yapılabilmekte,
- İşletim sisteminden kaynaklanabilecek sıkıntılara çabuk müdahale edilebilmekte,
- Merkezi olarak yama yönetimini yapılabilmekte,
- Aktif Dizin (kullanıcılar, bilgisayarlar, mekânlar,

yazıcılar gibi organizasyonun tüm bilgiler) yönetimi yapılabilmektedir.

17. *UYAP İç Güvenlik Sisteminde son kullanıcılar üzerinde hangi güvenlik önlemleri alınmıştır, açıklayınız?*

Cevap:

- Sistem üzerinde teknik destek veren kişiler haricinde tüm kullanıcılar bilgisayarlarında sınırlı kullanıcı olarak işlem yapabilmekteler.
- Her bilgisayar üzerinde temel işlemler haricinde kullanıcının işlem yapması engellenmiştir. (IP değiştirme, saat ayarlarını değiştirme v.b.)
- Her birimde yetki verilmiş olan teknik ofis elemanı sadece kendi biriminde yetkilidir. Başka bir birimde sadece sınırlı kullanıcı olarak işlem yapabilir.
- Kullanıcıların belirli aralıklar ile şifrelerini değiştirmeleri sağlanmaktadır.
- Şifre değiştirme işleminde aynı şifre kullanımı engellenmiştir.
- 3 kez hatalı şifre girilmesi durumunda kullanıcı hesabı kilitlenmekte ve yarım saat sonra otomatik olarak açılmaktadır.
- Şifrenin hangi bilgisayar üzerinden kilitlendiği bilgisi tespit edilebilmektedir.
- Kullanıcıların kullanmakta oldukları bilgisayarlara, daha önce belirlenmiş bilgisayar isimlendirme kuralına uygun olarak isim verilmektedir. İsimlendirme kuralına uymayan bilgisayarlar sistemden atılmaktadır.
- Bir bilgisayar etki alanından çıktıktan sonra aynı isim ile tekrar sisteme alınamamaktadır.
- Bilgisayarlara merkezi olarak güvenlik yamaları uygulanmaktadır.
- Kullanıcıların web browser üzerinden yaptıkları işlemlerde kullanıcı adı ve parola girilen ekranlar için parola ve kullanıcı adı hatırlama kapatılmıştır.
- Kullanıcıların tek bir proxy üzerinden çıkış yapmaları sağlanarak internet üzerinden gelen tehlikeler en aza indirilmiştir.
- Kullanıcı bilgisayarlarına merkezi olarak virüs tarama programı kurulumu yapılmakta ve yine merkezi olarak haftanın belirli günlerinde tüm bilgisayar üzerinde tarama yapılmaktadır.
- Kullanıcı bilgisayarlarında bulunan virüs programları merkezi olarak güncellenmektedir.

UYAP DIŞ GÜVENLİK SİSTEMİ

18. *UYAP sisteminde dış güvenlik kapsamında hangi güvenlik tedbirleri mevcuttur?*

Cevap:

- Intranet: UYAP kendi iç network (internet ağı) içinde çalışmaktadır.
- Noktadan Noktaya VPN (Virtual Private Network): Taşra birimleri, UYAP'a internet üzerinden erişir ama bu erişimi kendileri için özel olarak oluşturulmuş bir tünel içinden geçerek yaptıkları için talep ettikleri veya gönderdikleri bilgileri diğer internet kullanıcıları göremez.
- Firewall: iletişim 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 internet 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 imza
- Acil Durum Merkezi

UYAP BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS)

19. *"Kurumsal Bilgi Güvenliği" kavramı altında bir yönetim sistemi oluşturma yönünde yapılan çalışmalar hangi yıl hangi standartları ortaya çıkarmıştır?*

Cevap: 1993 yılında BS 7799 standardını, 2000 yılında ISO/IEC 17799 standardını ve 2006 yılında ISO/IEC 27001 standardını ortaya çıkarmıştır.

20. *Bilgi Güvenliği Yönetim Sisteminin (BGYS) sağlayacağı faydalar nelerdir?*

Cevap:

- Kurum çalışanlarının, kurumdan hizmet alan kişi ve kuruluşların ve iş ortaklarının, bilgi sistemi kaynaklarını kötü amaçlı olarak kullanmalarının engellenmesini sağlamak,
- Tehdit ve risklerin belirlenmesini ve etkin bir risk yönetimini sağlamak,
- Herhangi bir güvenlik ihlalinin engellenecek olması nedeniyle ortaya çıkabilecek yüksek maliyetlerden kurtulmayı sağlamak,
- İş sürekliliğini sağlamak,
- Kurum çalışanlarının güvenlik konusundaki farkındalık düzeyinin yükseltilmesi ve önemli güvenlik konularında bilgilendirilmesini sağlamak,
- Bilgi güvenliğinin dikkate alındığını, gerekli bilgi güvenliği adımların uygulandığını ve kontrollerin yapıldığı yani tüm seviyelerde bilgi güvenliğinin sağlandığını göstermek,
- Bilgi sistemlerinin güvenli olduğu konusunda çalışanlara ve iş ortaklarına kendilerinin güvende olduklarını hissettirmek,
- Kurumsal prestijin korunmasını ve artışını sağlamaktır.

UYAP BİLGİ SİSTEMİ NETWORK GÜVENLİK UYGULAMALARI

21. *Bakanlık bünyesinde kaç tane taşra birimi ve aktif kullanıcı vardır?*

Cevap: Bakanlık bünyesinde 1200'ü aşkın taşra birimi, birimlerde 40 000'i aşkın bilgisayar ve aktif kullanıcı bulunmaktadır.

22. *Bakanlık bünyesindeki sistemin güvenlik kontrolünün sağlanması için ne gibi önlemler alınmıştır?*

Cevap:

- Ana ve Yedek bağlantılar, Uç birim ve Merkezde kullanılan router cihazları ile temel olarak performans, süreklilik ve üst düzey güvenlik prensipleri esas alınarak iletişimin sağlandığı WAN ortamındaki trafik DMVPN (Dinamik Multipoint VPN) yapısı içerisinde uluslararası otoritelerce kabul edilen en üst düzey yöntem ve kripto algoritmalarıyla şifrelenmekte, özel olarak crypto authentication üretilen özel sertifika ile sağlanmakta
- Uç birim router cihazlarında uygulanan Access-List ler ile birim kullanıcılarının yalnızca belirli adreslerle iletişimine izin verilmekte ve kontrolsüz erişimler engellenerek izinsiz girişimler loglanmakta
- Aynı şekilde UYAP Sistem Merkezinde birim kullanıcılarına dair iletişim tekrar ve detaylı olarak firewall kontrolünden geçmekte, izinsiz erişimler engellenerek loglanmakta
- İzinli erişimler arasında atak vb. unsurlar için tüm trafik IPS kontrolünden geçerek engellenmekte ve loglanmakta
- Birim lokal networkündeki iletişim ile ilgili trafik akışları düzenli olarak gözlenmekte, izinli erişimler içerisinde yer alan olumsuz hareketler tespit edilerek müdahale edilmekte
- QOS uygulanarak merkezden sağlanan servisler ve bu servisleri sunan sunuculara dair trafik sınıflandırılmakta, sınıflandırılan her bir trafik için farklı bir policy uygulanmakta, herhangi bir servise dair trafiğin anormal seyri engellenmekte
- Tüm router cihazlarında güncel ve en uygun Ios/Firmware versiyonları kullanılmakta, bu cihazlar üzerinde güvenlik açığına neden olabilecek servisler ve tanımlamalar (CDP (Cisco Discovery Protocol), proxy-arp, redirection (Yönlendirme) vb) kullanılmamakta
- Router cihazlarına erişim yalnızca şifreli olarak SSH (Secure Shell/Güvenli Kabuk) protokolü ile ve yalnızca belirli adreslere sahip kişiler tarafından sağlanmakta diğer erişimler engellenmekte ve loglanmakta
- Yine router cihazlarına erişim hakkı TACACS (Terminal Access Controller Access Control System) servisi ile sağlanmakta, cihazlar üzerindeki hak ve tanımlama yetkileri kullanıcı seviyelerine göre belirlenmekte, cihazlar üzerindeki tüm işlem ve hareketler loglanmakta
- Yine SNMP (Simple Network Management Protocol - Basit Ağ Yönetim Protokolü) erişimleri yetkili ve yetkisiz seviyeler için sınıflandırılmakta, bu erişimlerin yalnızca belirli adresler üzerinden sağlanmasına izin verilmekte, izin verilmeyen ve engellenen tüm girişimler loglanmaktadır.

23. *Bakanlık bünyesindeki sistemin güvenlik kontrolünün sağlanması için internete dair ne gibi önlemler alınmıştır?*

Cevap:

- İnternet bağlantısını karşılayan router cihazı üzerinde atak önleyici özel modül, dedektörler ve tanımlamalar bulunmakta, mevcut ve tüm atak teknikleri engellenerek loglanmakta
- Atak önleyici modül ve detektör kontrolünden geçen trafik daha sonra firewall ve IPS kontrollerinden geçmekte
- Bu cihaza/cihazlara erişim ve yönetim hakkı, TACACS (Terminal Access Controller Access Control System) servisi ile yalnızca belirli adresler üzerinden ve yalnızca belirli kullanıcılar tarafından sağlanmaktadır.

24. *Bakanlık bünyesindeki sistemin güvenlik kontrolünün sağlanması için extranete dair ne gibi önlemler alınmıştır?*

Cevap:

- Her bir kurum bağlantısı extranet bağlantılarının sonlandığı router üzerinde tanımlanan VRF (Sanal router) tekniği ile birbirinden tamamen bağımsız olarak karşılanmakta,
- Her bir bağlantı ayrı ayrı üst düzey algoritmalar ile şifrelenmekte,
- Her bir kurumun kullandığı lokal IP subnetlerinin çakışabilmesi olasılığına karşı NAT uygulanmakta,
- Trafik akışları düzenli olarak gözlenmekte ve normal dışı durumlara müdahale edilmekte
- Extranet bağlantısını karşılayan router cihazına erişim ve yönetim hakkı TACACS servisi ile yalnızca belirli adresler üzerinden ve yalnızca belirli kullanıcılar tarafından sağlanmaktadır
- Kullanılan ürünler, iletişim teknikleri ve diğer yaklaşımlar yönünden Network Güvenliği konusunda dünya genelinde kabul gören tüm uygulamalar yakından takip edilmekte ve uygun olanları sisteme uyarlanmaktadır.

UYAP BİLGİ SİSTEMİ SİSTEM GÜVENLİK UYGULAMALARI

25. *UYAP bilgi sistemi sistem güvenlik uygulamaları altında sistemin clientlardan (istemci) korunması amacıyla neler gerçekleştirilmiştir?*
Cevap: Birbiri ardına akan paragraflar, bu paragrafların arasında yerleştirilmiş tablolar, grafikler, görüntüler ve benzeri görsel ögelerden oluşur.

- Uç noktadaki bütün clientlar üzerinde firewall, anti-virüs vardır.
- Bütün clientlara group policy üzerinden kısıtlamalar uygulanır.
- Clientların sisteme gereksiz gelmesi engellenir.
- Clientların kendi aralarında gereksiz trafiği engellenir.
- Clientlara QOS (Quality of Service) uygulanır.

26. *UYAP bilgi sistemi sistem güvenlik uygulamaları altında sistemin WAN saldırılarından korunması amacıyla neler gerçekleştirilmiştir?*
Cevap:

- Bütün dış sistem bağlantıları yedekli firewall üzerinden gelir.
- IPS (Intrusion Prevention Systems) atak önleme sistemi vardır.
- IDS (Intrusion Detection Sistem) saldırı tespit sistemi vardır.
- Dış sistem bağlantıları farklı networkler üzerinden yapılır.
- Bütün bağlantılar kriptoludur.
- VPN bağlantıları firewall üzerinde sonlandırılır.

27. *UYAP bilgi sistemi sistem güvenlik uygulamaları altında sistemin internet ortamından korunması amacıyla neler gerçekleştirilmiştir?*
Cevap:

- İnternet bağlantısı yedekli bir firewall katmanından geçer.
- WAN, LAN ve VPN bağlantıları için ayrı subnet kullanılır.
- 3 katmanlı bir yapı vardır.
- Her katmanda firewall bulunur.
- Her katmanda belli amaca hizmet eden sunucular bulunur.
- En kritik uygulamalar 3. katmandadır. (VT gibi)
- Her katmanda DMZ (De-Militarized Zone-Silahsızlandırılmış Alan) bölgeleri vardır.

28. *UYAP bilgi sistemi sistem güvenlik uygulamaları altında atak önleme amacıyla neler gerçekleştirilmiştir?*
Cevap:

- 3 farklı katmandaki sunuculara erişim ayrılmıştır.
- Erişime ulaşmadan önce IPS sistemi vardır.
- Bütün sunucular birbirinden izoledir.
- Bütün izole sunucu katmanları firewall arkasındadır.
- Yetkisiz erişimler kapalıdır.

UYAP VERİ GÜVENLİĞİ HAKKINDA YÖNETMELİK

29. *Veri Güvenliği Hakkında Yönetmelik hangi tarih ve sayılı kanun ile hazırlanmıştır?*
Cevap: Bu Yönetmelik, 15.05.2001 tarih ve 4674 sayılı Kanun ile 29.3.1984 tarihli ve 2992 sayılı Adalet Bakanlığı'nın Teşkilât ve Görevleri Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabulü Hakkında Kanun'a eklenen 22/A maddesi uyarınca hazırlanmıştır (Madde 3).

30. *UYAP Veri Güvenliği Hakkındaki Yönetmeliğin amacı nedir?*
Cevap: UYAP Veri Güvenliği Hakkındaki Yönetmeliğin amacı, Adalet Bakanlığına ait bilgi sistemlerinin internet üzerinden gelecek tehlikelerden korunması ve veri güvenliğinin sağlanması için alınacak güvenlik önlemlerine ilişkin usul ve esasları düzenlemektir.

PAROLA SEÇİMİ VE KULLANIMI

31. *Parola seçiminde alınması gereken tedbirler nelerdir?*
Cevap:

- Parolanız kesinlikle "adalet" olmamalıdır.
- Parolanız kesinlikle eş, çocuk veya herhangi bir yakın akrabanın adı, doğum tarihi, araba plakası, doğum yeri vs. gibi tahmin edilebilir bilgilerden oluşturulmamalıdır.
- Parolanız kesinlikle herhangi bir Türkçe veya Yabancı Dil Sözlüklerinde bulunan anlamlı bir kelime veya anlamlı bir kelimeden türetilmiş bir kelime veya özel isim olmamalıdır. (Örnek: Kayserili, Kayserilimisin, Diana, Superman, Galatasaray vs.)
- Uluslararası kabul görmüş ve güvenli sayılan parola; büyük harf, küçük harf, rakam veya özel işaretlerin en az üçünün birlikte kullanıldığı ve en az 7 haneden oluşan paroladır. (Örnek: At@TuRk, K1r$eH1R)
- Belirli aralıklarla mutlaka değiştirilmelidir.

YARDIM MASASI

32. *Yardım Masası kaç bölümden oluşmaktadır ve bu bölümleri isimleri nelerdir?*
Cevap: 3 bölümden oluşmaktadır. İsimleri; yazılım bölümü, donanım bölümü, parola işlemleri.

33. *Bilgi işlem Dairesi Başkanlığı Yardım Masası Şube Müdürlüğü hangi yıldan itibaren kaç alt sistem ve operatörle hizmet vermeye başlamıştır?*
Cevap: Bilgi işlem Dairesi Başkanlığı Yardım Masası Şube Müdürlüğü 2005 yılı temmuz ayından itibaren 7 alt sistemde 8 operatörle çalışmaya başlamıştır.

34. *Yardım Masasının Yazılım Bölümünün işlevi nedir?*
Cevap: Yazılım Bölümü: Her birim için ayrı ayrı oluşturulan modüllerde gelen hata ve düzeltme talepleri

sorumlu yardım masası operatörleri tarafından değerlendirildikten sonra yazılım grubuna yönlendirilerek çözüme kavuşturulmaktadır.

35. *Yardım Masasının Donanım Bölümünün işlevi nedir?*
Cevap: Donanım Bölümü: Telefonla ya da olay talebi ile gelen talepler ilgili birimin teknik ofisine yönlendirilir. Teknik ofis bir sorunla karşılaştığında ise donanım bölümüne ulaşarak taleplerini bildirmekte olup çözüm için telefon ile yönlendirilmektedirler. Uydu ya da UYAP bağlantısı ile ilgili bir problem bildirildiği takdirde, gerekli bilgiler alınarak Sistem bölümüne aktarılmaktadır.

36. *Yazılım Masasının Parola İşlemleri Bölümünün işlevi nedir?*
Cevap: Parola işlemleri: Domain (bilgisayar açılış), portal ve VPN sertifika şifreleri verilmektedir. Ayrıca mail hesaplarının oluşturulması için gelen taleplerde sistem bölümüne yönlendirilerek dönüş geldiğinde ilgili kullanıcıya şifre bilgisi verilmektedir.

37. *Yardım Masasının görevleri nelerdir?*
Cevap:

- Ulusal Yargı Ağının Adalet Bakanlığı'na 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,
- 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.

38. *Yardım Masasının hedefleri nelerdir?*
Cevap:

- 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 alt yapı ve program güncelleştirilmesinin yapılması
- Kullanıcıların yardım masasını daha etkin kullanımının sağlanmasıdır.