Çözümlerle Alıştırma Soruları

Bölüm 1

1. Güvenlik ve organizasyon hedeflerini ele almak için doğru yaklaşım nedir?

   a. Güvenlik ve organizasyon hedefleri ayrı ayrı geliştirilmelidir.

   b. Güvenlik, organizasyon hedeflerini yönlendirmelidir.

   c. Güvenlik, organizasyon hedeflerini desteklemelidir.

   d. Site güvenlik görevlisi, organizasyon hedeflerini onaylamalı veya reddetmelidir.

2. "Mesleki sertifika ve eğitim sağlanması yoluyla bilgi sistemi güvenliği uygulayıcıları arasında profesyonelliği teşvik edin" ifadesi a / a örneğidir:

   a. Görev beyanı

   b. Amaç

   c. Hedef

   d. Gereklilik

3. Risk yönetiminin iki bileşeni şunlardır:

   a. Risk değerlendirmesi ve risk analizi

   b. Güvenlik açığı değerlendirmesi ve risk tedavisi

   c. Risk değerlendirmesi ve risk azaltma

   d. Risk değerlendirmesi ve risk tedavisi

4. Bir güvenlik yöneticisinin, uygulamayı ve veritabanlarını korumak için hangi ek kontrollerin gerekebileceğini belirlemek için kritik bir iş uygulaması üzerinde bir risk değerlendirmesi yapması gerekir. Bu risk değerlendirmesini gerçekleştirmek için en iyi yaklaşım şudur:

   a. Yalnızca niteliksel bir risk değerlendirmesi gerçekleştirin

   b. Yalnızca nicel bir risk değerlendirmesi gerçekleştirin

c. Önce niteliksel bir risk değerlendirmesi yapın, ardından nicel bir risk değerlendirmesi yapın

d. Niceliksel bir risk değerlendirmesi yapın, ardından nitel bir risk değerlendirmesi yapın

5. Aşağıdakileri belirlemek için niteliksel bir risk değerlendirmesi kullanılır:

a. Güvenlik açıkları, tehditler ve karşı önlemler

b. Güvenlik açıkları, tehditler, tehdit olasılıkları ve karşı önlemler

c. Varlıklar, riskler ve azaltma planları

d. Güvenlik açıkları ve karşı önlemler

6. Belirli bir tehdidin etkisi şu şekilde tanımlanır:

a. Varlığı geri kazanmanın maliyeti

b. İlgili varlığı korumak için gereken maliyet

c. Gerçekleşmesi halinde tehdidin etkisi

d. Gerçekleşmesi halinde gelir kaybı

7. *Maruz kalma faktörü* olarak tanımlanır:

a. Bir varlığın değerinin belirli bir tehdit tarafından kaybedilmesi muhtemel olan kısmı

b. Tehdidin gerçekleşme olasılığı

c. Bir yıl içinde bir kayıp olma olasılığı

d. Tek bir kaybın maliyeti

8. Bir güvenlik yöneticisi, belirli bir varlık üzerinde nicel bir risk değerlendirmesi yapıyor. Güvenlik yöneticisi, belirli bir tehdide bağlı olarak tek bir kayıp için niceliksel kaybı belirlemek ister. Bunu hesaplamanın doğru yolu şudur:

a. Varlığın değerini maruziyet faktörüne bölün

b. Varlığın değeri ile yıllık meydana gelme oranını çarpın

c. Varlığın değerini tek kayıp beklentisiyle çarpın

d. Varlığın değerini maruz kalma faktörüyle çarpın

9. Bir güvenlik yöneticisi, belirli bir varlık üzerinde nicel bir risk değerlendirmesi yapıyor. Güvenlik yöneticisi, belirli bir tehdide dayalı olarak yıllık kaybı tahmin etmek ister. Bunu hesaplamanın doğru yolu şudur:

a. Tek kayıp beklentisi ile varlığın değeri ile çarpın Varlığın değerini

b. maruz kalma faktörüyle çarpın

c. Varlığın değeri ile maruziyet faktörü çarpı tek kayıp beklentisiyle çarpın

d. Tek kayıp beklentisi ile yıllık meydana gelme oranını çarpın

10. Yıllık kayıp beklentisi şu şekilde tanımlanır:

a. Tüm tehditlere dayalı olarak tüm varlıkların yıllık zarar tahmini

b. Tek bir tehdide dayalı olarak bir varlığın yıllık zarar tahmini

c. Tüm tehditlere dayalı olarak bir varlığın yıllık zarar tahmini

d. Tek bir tehdide dayalı olarak tüm varlıkların yıllık zarar tahmini

11. Yıllık zarar beklentisi, aşağıdaki formül kullanılarak hesaplanır:

a. ALE = ARO x SLE

b. ALE = EF x SLE

c. ALE = ARO x AV

d. ALE = ARO / SLE

12. Bir risk yöneticisi, 4000 $ değerindeki bir varlık için bir risk analizini tamamladı. İki tehdit tespit edildi; bir tehdit için ALE 400 dolar ve ikinci tehdit için ALE 500 dolar. Kuruluşun bir yıl boyunca tahmin etmesi gereken kayıp miktarı nedir?

a. 450 ABD doları

b. $500 dolar

c. 900 $

d. 100 $

13. Risk tedavisi için seçenekler şunlardır:

a. Risk azaltma, risk varsayımı, riskten kaçınma ve risk kabulü

b. Risk kabulü, risk azaltma, risk transferi ve risk azaltma

c. Risk kabulü, risk azaltma ve risk transferi

d. Risk kabulü, riskten kaçınma, risk azaltma ve risk transferi

14. Bir kuruluş yakın zamanda bir risk değerlendirmesini tamamladı. Risk değerlendirmesindeki bulgulara dayanarak, kuruluş olası kayıpları karşılamak için sigorta satın almayı seçti. Bu yaklaşım şu şekilde bilinir:

a. Risk transferi

b. Riskten kaçınma

c. Risk kabulü

d. Risk azaltma

15. Bir risk değerlendirmesini tamamladıktan sonra, bir kuruluş tespit edici ve önleyici kontroller ekleyerek riski azaltmayı başardı. Ancak, bu kontroller tüm riski ortadan kaldırmadı. Kuruluşun kalan riski ele almak için ne gibi seçenekleri var?

a. Kabul edin, kaçının, azaltın veya aktarın

b. Yok - kuruluş riski kabul etmelidir

c. Kuruluş riski kabul etmeli veya devretmelidir

d. Geçerli değil: kalan risk daha fazla tedavi edilemez

16. Bir elektrik kesintisi durumunda binanın kapı giriş sisteminden gelen sinyalleri göz ardı edecek şekilde bir güvenlik kapısı tasarlanmıştır. Bu şu şekilde bilinir:

a. Yumuşak başarısız

b. Açık başarısız

c. Başarısız kapatıldı

d. Güvenli başarısız

17. CIA şu şekilde bilinir:

a. Gizlilik, Bütünlük ve Kullanılabilirlik

b. Bilgisayarlar, Bilgiler ve Varlıklar

c. Uygulamalarda Güven

d. Kontroller, Bütünlük ve Kullanılabilirlik

18. Bir kuruluş, bir çalışan tarafından bir spam iletisiyle kötü amaçlı yazılım indirildiğinde bir virüs salgını yaşadı. Kuruluş aşağıdaki güvenlik ilkesini izlemiş olsaydı bu salgın gerçekleşmeyebilirdi:

a. Heterojenlik

b. Kale

c. Bütünlük

d. Derinlemesine savunma

19. Bir kuruluş, politika, risk yönetimi, standartlar ve süreçler gibi güvenlikle ilgili etkinliklerin güçlü, yönetim odaklı bir modeline sahiptir. Bu model daha çok şu şekilde bilinir:

a. Risk yönetimi

b. Güvenlik gözetimi

c. Güvenlik yönetişimi

d. Güvenlik kontrolü

20. "Bilgi sistemleri güçlü parolalar gerektirecek şekilde yapılandırılmalıdır" ifadesi a / a örneğidir:

a. Güvenlik gereksinimi

b. Güvenlik Politikası

c. Güvenlik hedefi

d. Güvenlik kontrolü

21. Bir kuruluş bir uygulama satın almak istiyor ve bir ürünü değerlendirmek ve seçmek için resmi bir satın alma sürecinden geçiyor. Kuruluş, seçilen uygulamanın güvenlikle ilgili uygun özelliklere sahip olduğundan emin olmak için hangi belgeleri kullanmalıdır?

a. Güvenlik kuralları

b. Güvenlik politikaları

c. Güvenlik gereksinimleri

d. İşlevsel gereksinimler

22. Bir güvenlik yöneticisi bir veri sınıflandırma politikası geliştiriyor. Politikada hangi unsurların olması gerekiyor?

a. Hassasiyet seviyeleri, işaretleme prosedürleri, erişim prosedürleri ve kullanım prosedürleri

b. Etiketleme prosedürleri, erişim prosedürleri ve kullanım prosedürleri

c. Hassasiyet seviyeleri, erişim prosedürleri ve kullanım prosedürleri

d. Hassasiyet seviyeleri ve kullanım prosedürleri

23. Daha önce sabıka geçmişi olan bir çalışanın işine son verildi. Eski çalışan birkaç hassas belgeyi haber medyasına sızdırdı. Bunu önlemek için kuruluşun sahip olması gerekenler:

a. Erişim günlükleri incelendi

b. Çalışanın hassas bilgilere erişimini kısıtladı

c. İmzalı bir ifşa etmeme beyanı elde edildi

d. Çalışanı işe almadan önce bir arka plan doğrulaması gerçekleştirdi

24. Bir kuruluş, yakın zamanda mali uygulamalarının denetiminden geçmiştir. Denetim raporu, uygulamanın BT desteğiyle ilgili birkaç görev ayrılığı sorunu olduğunu belirtti. Ne anlama geliyor?

a. BT personelinin finansal verilere erişimi olmamalıdır.

b. Personelin görevleri resmi olarak tanımlanmamıştır.

c. BT'nin iş rotasyonu uygulamasına başlaması gerekiyor.

d. BT'deki bireylerin çok fazla rolü veya ayrıcalığı vardır.

25. Bir kuruluş, görevlerini yerine getirmek için bilgisayar kullanan yüzlerce ofis çalışanı istihdam etmektedir. Çalışanları güvenlik sorunları hakkında bilgilendirmek için en iyi plan nedir?

a. Çalışan el kitabına güvenlik politikasını dahil edin

b. İşe alma sırasında ve sonrasında yıllık olarak güvenlik bilinci eğitimi uygulayın

c. İşe alma sırasında güvenlik bilinci eğitimi uygulayın

d. Çalışanların kurumsal güvenlik politikasını imzalamasını zorunlu kılın

Bölüm 2

26. Hassas bilgileri işleyen bir bilgi sistemi, herhangi bir kullanıcıdan geçerli bir kullanıcı kimliği ve güçlü bir parola gerektirecek şekilde yapılandırılır. Bu bilgileri kabul etme ve doğrulama süreci şu şekilde bilinir:

a. Doğrulama

b. Güçlü kimlik doğrulama

c. İki faktörlü kimlik doğrulama

d. Tek seferlik

27. İki faktörlü kimlik doğrulamanın sıradan kimlik doğrulamaya tercih edilmesinin nedeni şudur:

a. İki faktörlü kimlik doğrulamanın kırılması daha zordur

b. Kullanıcının bildiği bir şeye dayanır

c. Kullanıcının sahip olduğu bir şeye dayanır

d. İki faktörlü kimlik doğrulama, daha güçlü şifreleme algoritmaları kullanır

28. Bir bilgi sistemi, "kullanıcının ne olduğuna" dayalı olarak bir kullanıcının kimliğini doğruladığında, bu aşağıdakilerin kullanımına atıfta bulunur:

a. Kullanıcının iş unvanına dayalı yetkilendirme

b. Rol tabanlı kimlik doğrulama

c. İki faktörlü kimlik doğrulama

d. Biyometrik kimlik doğrulama

29. Kullanıcı kimliğine ve parolaya dayalı olarak kullanıcıların kimliğini doğrulayan bir bilgi sisteminde, şifreli parolayı depolamak yerine parolanın bir karmasını depolamanın birincil nedeni şudur:

a. Hiç kimse, sistem yöneticileri bile parolayı türetemez

b. Hashing algoritmaları, şifreleme algoritmalarından daha az CPU-yoğunlukludur

c. Karma parolalar, şifrelenmiş parolalara göre daha az depolama alanı gerektirir

d. Destek personeli, hashing uygulandığında bir kullanıcının parolasını daha kolay sıfırlayabilir

30. Kullanıcılara güçlü parolalar kullanmalarının söylenmesinin temel nedeni:

a. Ek tuş vuruşları nedeniyle güçlü bir parola "omuz sörfü" yapmak daha zordur

b. Güçlü parolaları başkalarının tahmin etmesi daha zordur Zayıf

c. parolalar sözlük saldırılarına karşı hassastır

d. Doğum günleri, eşler ve evcil hayvan isimleri gibi kolayca keşfedilen gerçeklere dayanan şifreler kolayca tahmin edilebilir

31. İki faktörlü kimlik doğrulama aracı olarak dijital sertifikaların kullanılmasının bir dezavantajı şu DEĞİLDİR:

a. Dijital sertifikalar farklı türdeki makinelerde taşınabilir olmayabilir

b. Sertifikanın kilidini açmak için kullanılan şifre zayıf olabilir ve kolayca tahmin edilebilir

c. Sertifikayı çalıp başka bir bilgisayarda kullanmak mümkün olabilir

d. Kolayca klonlanamayan belirteçler ve akıllı kartların aksine, dijital bir sertifika teorik olarak kopyalanabilir

32. Akıllı kart, iki faktörlü kimlik doğrulamanın iyi bir şeklidir çünkü:

a. Mikroçip üzerinde klonlamaya veya çatlamaya dayanıklı bir sertifika içerir

b. Bina giriş anahtar kart sistemleri için bir yakınlık kartı olarak ikiye katlanabilir

c. Bir jeton gibi dahili güce dayanmaz

d. Akıllı kart taşınabilir ve başkalarına ödünç verilebilir

33. İki faktörlü kimlik doğrulamayı uygulayan kuruluşlar, genellikle yeterince planlama yapmazlar. Bunun bir sonucu:

a. Bazı kullanıcılar jetonlarını, akıllı kartlarını veya USB anahtarlarını kaybedecek

b. Bazı kullanıcılar tokenlerini, akıllı kartlarını veya USB anahtarlarını bilgisayarlarında saklayacak ve böylece iki faktörlü kimlik doğrulamanın avantajlarından birini ortadan kaldıracaktır.

c. Kullanıcılar iki faktörlü kimlik doğrulamayı nasıl kullanacaklarını anlamakta güçlük çekecekler

d. Uygulama ve destek maliyeti, ürünün kendi maliyetini kolayca aşabilir

34. Avuç içi taraması, parmak izi taraması ve iris taraması aşağıdakilerin biçimleridir:

a. Güçlü kimlik doğrulama

b. İki faktörlü kimlik doğrulama

c. Biyometrik kimlik doğrulama

d. Tek seferlik

35. Yeni taramaların sonuçlarını bir kullanıcının profiline dahil eden bir biyometrik kimlik doğrulama sisteminin aşağıdakileri yapma olasılığı daha düşüktür:

a. Daha düşük bir Yanlış Kabul Oranına sahip olun

b. Kullanıcının biyometrikleri zaman içinde yavaşça değiştiği için gelecekteki kimlik doğrulama girişimlerini reddedin

c. Kullanıcıları doğru şekilde tanımlayın ve kimliklerini doğrulayın

d. Bir sahtekarı reddetmek

36. Retina taramasının biyometrik kimlik doğrulama yöntemi olarak kullanılması, aşağıdaki nedenlerden dolayı popülerlik kazanmamıştır:

a. Karanlık bir odada retina taramasının kullanılması sakıncalıdır.

b. Birçok kullanıcı bir taramanın tamamlanmasına yetecek kadar gözlerini açık tutamaz

c. Kullanıcılar, gözlerini biyometrik tarama cihazına çok yakın tutmaktan rahatsız oluyorlar

d. İnsan retinası zamanla önemli ölçüde değişir

37. Biyometrik kimlik doğrulama yöntemi olarak ses tanımanın ölçülmesi zordur, çünkü:

a. Mevcut sağlık ve solunum hızı gibi birçok faktör, örneklemeyi zorlaştırıyor

b. Bilgisayarlar henüz bir ses baskısını yeterince örneklemek için yeterince hızlı değil Ses

c. tanıma, aksanları iyi yönetmiyor

d. Sabırsızlık, ses kalıplarını değiştirerek Yanlış Red Oranlarının artmasına neden olur

38. Çapraz Hata Oranı (CER) ile ilgili aşağıdaki ifadelerden hangisi doğrudur:

a. Yanlış Kabul Oranının% 50'nin altına düştüğü nokta budur

b. Bu, Yanlış Red Oranının% 50'nin altına düştüğü noktadır

c. Bu, Yanlış Reddetme Oranı ve Yanlış Kabul Oranının% 100'e eklendiği noktadır.

d. Bu, Yanlış Reddetme Oranı ile Yanlış Kabul Oranının eşit olduğu noktadır.

39. bir güvenlik mühendisi yakın zamanda bir biyometrik sistem kurdu ve ayarlamak için. Şu anda biyometrik sistem çok sayıda geçerli, kayıtlı kullanıcıyı reddediyor. Güvenlik mühendisinin ne ayarlaması gerekiyor?

a. Yanlış Kabul Oranını Artırın

b. Yanlış Kabul Oranını Düşürün

c. Yanlış Reddetme Oranını Artırın

d. Yanlış Reddetme Oranını Azaltın

40. Bir güvenlik mühendisi, merkezi kimlik doğrulaması yapacak bir yazılım ürünü için teklif istiyor. Mühendis şu ana kadar iki ürün buldu: biri LDAP'ye, diğeri TACACS'a dayalı. Aşağıdaki ifadelerden hangisi en iyi yaklaşımdır?

a. LDAP tabanlı ürünü seçin

b. TACACS tabanlı ürünü düşünmeyin, LDAP tabanlı ürünü düşünmeyin ve diğer ürünleri aramaya devam edin

c. TACACS tabanlı ürünü seçin

d. TACACS tabanlı ürünü düşünün ve TACACS'a dayalı diğer ürünleri aramaya devam edin

41. Aşağıdakilerden hangisi bir kimlik doğrulama protokolü DEĞİLDİR:

a. Hafif Dizin Kimlik Doğrulama Protokolü

b. Çap

c. YARIÇAP

d. Basit Dizin Erişim Protokolü

42. Bir davetsiz misafir, orada saklanan bilgileri çalmak için bir uygulamaya girmek ister. Uygulama güçlü kimlik doğrulama kullandığından, saldırganın izleyeceği en olası yaklaşım nedir?

a. Sözlük saldırısı

b. Kötü amaçlı kod saldırısı

c. Uygulama baypas saldırısı

d. Parola tahmin saldırısı

43. Kimlik doğrulama, şifreleme ve ACL'ler aşağıdakilere örnektir:

a. Derinlemesine savunma

b. Dedektif kontrolleri

c. İdari kontroller

d. Teknik kontroller

44. Kontrol kategorileri şunlardır:

a. Dedektif, caydırıcı, önleyici, düzeltici, iyileştirici ve telafi edici

b. Dedektif, önleyici ve caydırıcı

c. Teknik, mantıksal ve fiziksel

d. Dedektif, önleyici, iyileştirici ve telafi edici

45. Video gözetimi, hangi tür kontrollerin bir örneğidir:

a. Dedektif ve caydırıcı

b. Sadece dedektif

c. Sadece caydırıcı

d. Önleyici

46. Arabellek taşması, SQL enjeksiyonu ve yığın parçalama şu örneklerdir:

a. Güvenlik açıkları

b. İstismarlar

c. Girdi saldırıları

d. Enjeksiyon saldırıları

47. Bir kuruluş, eski masaüstü bilgisayarlarını şaşırtmaktadır. Veri kalitesiyle ilgilenen kuruluş ilk önce hangi önlemleri almalıdır?

a. Sabit sürücüleri silin

b. Sabit sürücüleri biçimlendirin

c. TEMPEST korumasını etkinleştirin

d. Bilgisayarların RAM'ini temizleyin

48. Sosyal mühendisliğe karşı en iyi savunma nedir?

a. Casus yazılım filtreleri

b. Güvenlik duvarları

c. Veri sızıntısı koruması (DLP)

d. Güvenlik bilinci eğitimi

49. İşaretler, korumalar, bekçi köpekleri ve görünür uyarılar aşağıdakilere örnektir:

a. İdari kontroller

b. Önleyici kontroller

c. Caydırıcı kontroller

d. Dedektif kontrolleri

50. Önleyici kontrollerin dedektif kontrollere tercih edilmesinin nedeni şudur:

a. Önleyici kontroller daha az maliyetlidir

b. Dedektif kontroller aslında istenmeyen faaliyetleri durdurmaz

c. Dedektif kontroller daha fazla kaynak gerektirir

d. Önleyici kontroller istenmeyen aktiviteyi tespit etmez

Bölüm 3

51. Bir kuruluşun dağıtılmış bir uygulamayı dikkate almasının bir nedeni şudur:

a. Bazı bileşenlerin çalıştırılması daha kolaydır

b. Dağıtılmış uygulamalar, diğer uygulama türlerine göre daha basit bir mimariye sahiptir

c. Bazı uygulama bileşenleri başka kuruluşlara aittir ve başka kuruluşlara aittir

d. Dağıtılmış uygulamaların güvenliğini sağlamak daha kolaydır

52. Aşağıdakilerin tümü, kendinden imzalı SSL sertifikalarını kullanmanın avantajları HARİÇ:

a. Sunucu kimlik doğrulaması

b. Daha az maliyet

c. Oluşturması daha kolay

d. Çatlamak daha zor

53. NOP kızak saldırısına karşı en iyi savunma:

a. Güvenlik duvarı

b. Anti-virüs

c. Strcpy () işlevi

d. Giriş sınırı kontrolü

54. Bir nesnenin içerdiği talimatlar şu şekilde bilinir:

a. Sınıf

b. Firmware

c. Kod

d. Yöntem

55. Yığına bir "kanarya" değeri koymanın amacı şudur:

a. Sözlük saldırısını tespit etmek için

b. Bir yığın parçalama saldırısını tespit etmek için

c. Parametre kurcalamayı tespit etmek için

d. Komut dosyası yerleştirmeyi tespit etmek için

56. "Güvenli diller" ve "güvenli kitaplıklar" sözde çünkü:

a. Bazı giriş saldırı biçimlerini otomatik olarak algılarlar

b. Parametrelerin kurcalanmasını otomatik olarak algılarlar

c. Komut dosyası yerleştirmeyi otomatik olarak algılarlar

d. Kötü amaçlı yazılım saldırılarını otomatik olarak tespit ederler

57. Aşağıdakiler bir bilgisayar virüsünün özellikleridir, HARİÇ:

a. Polimorfik

b. İndirilebilir

c. Kendi kendine yayılan

d. Spam'e gömülü

58. Rootkit'leri tespit etmek zor olabilir çünkü:

a. Şifrelenmişler

b. Polimorfiktirler

c. Sabit sürücü yerine ROM'da bulunurlar

d. Kendilerini saklamak için teknikler kullanırlar

59. Sahte "A" kayıtlarını yerleştirmek için bir DNS sunucusuna yapılan saldırı, aşağıdakilerin karakteristiğidir:

a. Pharming saldırısı

b. Kimlik avı saldırısı

c. Balina avı saldırısı

d. Spim saldırısı

60. Tarayıcı Yardımcı Nesnesini (BHO) dijital olarak imzalamanın amacı şudur:

a. Kökenini kanıtlamak için

b. Kötü niyetli olmadığını kanıtlamak için

c. Güvenilir olabileceğini kanıtlamak için

d. Düzgün indirildiğini kanıtlamak için

61. Bir kuruluş, İnternet web uygulamasına SQL ve komut dosyası yerleştirme saldırılarını önlemek istemektedir. Organizasyon a / a uygulamalıdır:

a. Saldırı tespit sistemi

b. Güvenlik duvarı

c. Uygulama güvenlik duvarı

d. SSL sertifikası

62. Kötü amaçlı yazılımdan koruma için kapsamlı bir savunma stratejisi önerilmektedir, çünkü:

a. Çok sayıda kötü amaçlı yazılım saldırı vektörü var

b. Anti-virüs yazılımı genellikle son kullanıcı iş istasyonlarında zahmetlidir

c. Kötü amaçlı yazılım, SSL iletimlerinde gizlenebilir

d. Kullanıcılar, iş istasyonlarında kötü amaçlı yazılımdan korunmayı önleyebilir

63. İş istasyonu tabanlı anti-virüs kullanımının birincil avantajı şudur:

a. Virüs imza güncellemeleri daha seyrek gerçekleştirilebilir

b. Virüs imza güncellemeleri daha sık gerçekleştirilebilir

c. Kullanıcı yapılandırmasını kontrol edebilir

d. Bu yaklaşım, hepsi olmasa da çoğu saldırı vektörüne karşı savunma sağlayabilir.

64. Bir güvenlik duvarının birincil amacı:

a. Bir sunucuyu kötü niyetli trafikten korumak için

b. Kötü amaçlı kodu engellemek için

c. Ağlar arasındaki trafiği kontrol etmek için

d. Bir DMZ ağı oluşturmak için

65. Aşağıdakiler, iş istasyonu kullanıcıları için ayrıcalık düzeyini düşürmek için geçerli nedenlerdir, HARİÇ:

a. Kullanıcıların sistem yapılandırmalarını değiştirememesi nedeniyle daha düşük destek maliyetleri

b. Tam disk şifreleme ihtiyacının azalması

c. Kötü amaçlı yazılımın etkisinde azalma

d. Kullanıcılar güvenlik kontrollerini kurcalayamadığı için artırılmış güvenlik

66. Bir sistem yöneticisinin bir sunucuyu sağlamlaştırması gerekiyor. En etkili yaklaşım şudur:

a. Güvenlik yamalarını kurun ve bir güvenlik duvarı kurun

b. Gereksiz hizmetleri kaldırın, gereksiz hesapları kaldırın ve bir güvenlik duvarı yapılandırın

c. Gereksiz hizmetleri kaldırın, kullanılmayan bağlantı noktalarını devre dışı bırakın ve gereksiz hesapları kaldırın

d. Güvenlik yamalarını yükleyin ve gereksiz hizmetleri kaldırın

67. Girdi saldırılarına karşı en etkili karşı önlemler şunlardır:

a. Giriş alanı filtreleme, uygulama güvenlik duvarı, uygulama güvenlik açığı taraması ve geliştirici eğitimi

b. Giriş alanı filtreleme, uygulama güvenlik duvarı ve izinsiz girişi önleme sistemi

c. Giriş alanı filtreleme, uygulama güvenlik duvarı, izinsiz giriş tespit sistemi ve etik korsanlık

d. Uygulama güvenlik duvarı, saldırı tespit sistemi ve geliştirici eğitimi

68. "Nesnenin yeniden kullanımı" terimi aşağıdakileri ifade eder:

a. Kötü amaçlı yazılımlar tarafından çalışan süreçlerdeki zayıflıklardan yararlanmak için kullanılan bir yöntem

b. Kalan bilgi işlem kaynaklarının başka amaçlar için kullanılması

c. Uygulama kodunu yeniden kullanma yeteneği

d. Diğer işlemlerle ilişkili artık verileri bulabilen ve kullanabilen işlemler

69. Bir güvenlik değerlendirmesi, bir uygulamada arka kapılar keşfetti ve güvenlik yöneticisinin gelecekte arka kapıları tespit etmek ve kaldırmak için bir plan geliştirmesi gerekiyor. Seçilmesi gereken en etkili karşı önlemler şunlardır:

a. Uygulama güvenlik duvarları

b. Kaynak kodu kontrolü

c. Dış kod incelemeleri

d. Eş kodu incelemeleri

70. Bir uygulamaya güvenlik getirmenin en iyi zamanı:

a. Uygulama

b. Tasarım

c. Geliştirme

d. Test yapmak

71. Bir kullanıcı, Bill, bir web sitesinde, şüphelenmeyen kullanıcıların bağlantıyı tıklarlarsa Bill'e para transfer etmelerine neden olan bir bağlantı yayınladı. Bağlantı, yalnızca bağlantının hedefi olan bankada kimliği doğrulanmış kullanıcılar için çalışacaktır. Bu şu şekilde bilinir:

a. Siteler arası istek sahteciliği

b. Siteler arası komut dosyası oluşturma

c. Bozuk kimlik doğrulama

d. Tekrar saldırı

72. Komut dosyası yerleştirme saldırılarına karşı en etkili önlem nedir?

a. Durum bilgisi olan denetim güvenlik duvarı

b. Son kullanıcının tarayıcı yapılandırmasında sunucu tarafı komut dizisine izin verme

c. Tüm giriş alanlarındaki komut dosyası karakterlerini filtreleyin

d. Son kullanıcının tarayıcı yapılandırmasında istemci tarafı komut dosyalarına izin verme

73. Bir veritabanı yöneticisi (DBA), hangi kullanıcıların hangi verilere erişebileceğini kontrol etmeyi içeren güvenlik politikasını yürütmekten sorumludur. DBA'dan, bazı veritabanı tablolarındaki bazı alanların bazı yeni kullanıcılar tarafından görülebilmesi istenmiştir. DBA'nın alacağı en iyi hareket tarzı nedir?

a. Sütun tabanlı erişim kontrolleri uygulayın

b. Tabloyu, yalnızca kullanıcıların görmesine izin verilen alanlar dahil olmak üzere bir veri ambarına aktarın

c. Yalnızca kullanıcıların görmesine izin verilen alanlar dahil olmak üzere tabloyu klonlayın

d. Yalnızca kullanıcıların görmesine izin verilen alanları içeren bir görünüm oluşturun

74. Veri Kontrol Dilinin amacı:

a. Bir veritabanındaki verileri hangi kullanıcıların görüntüleyebileceğini ve işleyebileceğini tanımlayın

b. İlişkisel bir veritabanında veri yapılarını tanımlayın

c. Nesne yönelimli bir veritabanında veri yapılarını tanımlayın

d. İlişkisel bir veritabanındaki verileri alın, ekleyin, silin ve güncelleyin

75. Bir uygulamada meydana gelen tüm önemli olayların listesi şu şekilde bilinir:

a. Denetim günlüğü

b. Yeniden oynatma günlüğü

c. Aktarma dosyası

d. Veri dökümü

4. Bölüm

76. Afetleri doğal veya insan yapımı olarak sınıflandırmanın birincil nedeni şudur:

a. Olası etkilerini doğru bir şekilde belirlemek için

b. Gerçekleşme olasılıklarını doğru bir şekilde belirlemek için

c. Daha iyi anlamak için farklı olay türlerini sınıflandırmak

d. Hangi acil durum planlarının gerçekleştirilmesi gerektiğini belirlemek için

77. İş sürekliliği ve felaket kurtarma planlaması amacıyla, "felaket" tanımı şu şekildedir:

a. Bir kuruluşun çalışmaya devam etme yeteneğini bozan herhangi bir olay

b. Bir kuruluşun çalışmaya devam etme yeteneğini bozan herhangi bir doğal olay

c. Bir kuruluşun çalışmaya devam etme yeteneğini bozan herhangi bir insan yapımı olay

d. Bir kuruluşun BT sistemlerinin çalışmaya devam etme yeteneğini bozan herhangi bir olay

78. Bir pandeminin bir organizasyon üzerindeki birincil etkisi:

a. Kamu hizmetlerinde önemli aksaklıklar

b. Ulaşım sistemlerinde önemli aksaklıklar

c. Hizmet talebini azaltan çok sayıda zayiat

d. Kuruluşun hizmet sunma kabiliyetini etkileyen uzun süreli çalışan devamsızlığı

79. Ticari faaliyetlerin sürdürülmesiyle ilgili faaliyet:

a. Acil Müdahale Prosedürleri

b. Felaket Kurtarma Planlaması

c. İş Sürekliliği Planlaması

d. İş Etki Analizi

80. Bir DRP projesinin yönetici desteği ve onayı almasının ana nedeni şudur:

a. Bir DRP projesi çok pahalıdır

b. Bir DRP projesi, kaynakların tahsisinde önemli ayarlamalar gerektirir

c. Bir DRP projesi, tüm kapsam içi BT sistemlerinin yeniden tasarlanmasını gerektirir

d. Bir DRP projesi, tüm kapsam içi iş süreçlerinin yeniden tasarlanmasını gerektirir

81. Bir kuruluş, ilk felaket kurtarma planlama projesine başlamak üzeredir. Proje yöneticisi, proje ekip üyelerinin seçiminden sorumludur. Bu proje için hangi personel seçilmelidir?

a. Proje, dış kaynaklı teknik uzmanlar kullanmalıdır

b. En az deneyimli ekip üyeleri

c. En deneyimli ekip üyeleri

d. Proje, dış kaynaklı felaket kurtarma planlama uzmanları kullanmalıdır

82. Bir felaket kurtarma planlama projesinin başlangıcında, proje ekibi kuruluşun en önemli iş süreçlerinin tümünün bir listesini derleyecektir. Projenin bu aşaması şu şekilde bilinir:

a. İş Etki Analizi

b. Risk analizi

c. İş Süreçleri Analizi

d. Maksimum tolere edilebilir kesinti süresinin (MTD) belirlenmesi

83. Bir afet kurtarma planlama projesi hangi sırayla gerçekleştirilmelidir?

a. İş Etki Analizi, Maksimum Tolere Edilebilir Kapalı Kalma Süresi, Kurtarma Noktası Hedefi, Kurtarma Süresi Hedefi, eğitim, test

b. İş süreçlerini araştırın, tehdit ve risk analizi, kurtarma hedefleri geliştirin, kritiklik analizi

c. Proje planı, risk değerlendirmesi, etki beyanları, kritiklik analizi, kurtarma hedefleri, test kurtarma planları

d. Proje planı, İş Etki Analizi, kurtarma planları geliştirme, personeli eğitme, test kurtarma planları

84. Olağanüstü durum kurtarma ve iş sürekliliği planlamasından elde edilen faydalar, aşağıdakilerin tümünü içerir:

a. Geliştirilmiş sistem dayanıklılığı

b. Süreç iyileştirmeleri

c. Geliştirilmiş pazar avantajı

d. Geliştirilmiş performans

85. BCP ve DRP testlerinin türleri şunlardır:

a. Belge incelemesi, gözden geçirme, paralel test, kesme testi

b. Belge incelemesi, izlenecek yol, simülasyon, paralel test, kesme testi

c. Belge incelemesi, gözden geçirme, akıl sağlığı testi, paralel test, kesme testi

d. İzlenecek yol, simülasyon, paralel test, kesme testi, canlı test

86. Bir kesme testinin amacı:

a. Üretim sistemleri yerine yedek sistemler üzerinde canlı iş işlemleri gerçekleştirme yeteneğini belirlemek

b. Bir kurtarma testinin kesintiye uğrama yeteneğini belirlemek için

c. Üretim sistemleri ve yedekleme sistemleri üzerinde aynı anda canlı iş işlemleri yapabilme yeteneğini belirlemek

d. Bir kurtarma ekibinin son dakika değişikliği için yeteneğini belirlemek için

87. Paralel testin amacı:

a. Üretim sistemleri yerine yedek sistemler üzerinde canlı iş işlemleri gerçekleştirme yeteneğini belirlemek

b. Bir kurtarma testinin kesintiye uğrama yeteneğini belirlemek için

c. Üretim sistemleri ve yedekleme sistemleri üzerinde aynı anda canlı iş işlemleri yapabilme yeteneğini belirlemek

d. Bir kurtarma ekibinin son dakika değişikliği için yeteneğini belirlemek için

88. Bir kesme testiyle ilgili en büyük risk:

a. Yedekleme sunucuları düzgün çalışmazsa, test başarısız olur

b. Bir kesme testi, geçişi değil yalnızca canlı yükü test eder

c. Kesme testi, canlı yükü değil yalnızca geçişi test eder

d. Yedekleme sunucuları düzgün çalışmıyorsa, kritik iş süreçleri başarısız olabilir

89. Bir proje ekibi kuruluşun iş sürekliliği planını oluşturmayı henüz tamamladı. Aşağıdaki testlerden hangisi önce yapılmalıdır?

a. İzlenecek yol

b. Simülasyon

c. Paralel test

d. Kesme testi

90. Olağanüstü durumdan kurtarma yeteneği oluşturan bir kuruluşun, 40 saatlik RPO ve 24 saatlik RTO'nun yeni kurtarma gereksinimlerini karşılamak için uygulama sunucularını yeniden tasarlaması gerekir. Aşağıdaki yaklaşımlardan hangisi bu hedefi en iyi şekilde karşılayacaktır?

a. Çoğaltmalı Aktif / Pasif sunucu kümesi

b. Teyp yedekleme ve sıcak bir siteye geri yükleme

c. Teyp yedekleme ve soğuk bir siteye geri yükleme

d. Paylaşılan depolamaya sahip sunucu kümesi

91. Bir sunucu kümesinin amacı aşağıdakilerin tümünü içerir, HARİÇ:

a. Bir uygulamanın kullanılabilirliğini iyileştirin

b. Bir uygulamanın kapasitesini artırın

c. Bir uygulamanın veri depolamasını artırın

d. Hata toleransı sağlayın

92. Site dışı ortam depolamanın amacı:

a. Afet durumunda medyayı hasardan korumak için

b. Medyayı hırsızlığa karşı korumak için

c. Yerinde olmayan ek depolama sağlamak için

d. Medya korumasına yönelik yasal gereklilikleri karşılamak için

93. Bir felaket kurtarma planlama projesi yürüten bir kuruluş, bir elektrik şebekesi arızası durumunda, on güne kadar yerinde elektrik gücüne sahip olması gerektiğini belirlemiştir. Bu gereksinim için en iyi yaklaşım şudur:

a. Kesintisiz güç kaynağı (UPS) ve güç dağıtım birimi (PDU)

b. Elektrik jeneratörü

c. Kesintisiz güç kaynağı (UPS)

d. Kesintisiz güç kaynağı (UPS) ve elektrik jeneratörü

94. Afete müdahalede ilk öncelik şu olmalıdır:

a. Yedekleme ortamı

b. Kağıt kayıtları

c. Personel güvenliği

d. Uzaktan erişim

95. Aşağıdakilerden hangisi, afetle ilgili bir acil durumda bildirilecek taraflar listesinde OLMAYACAKTIR:

a. Sivil yetkililer

b. Araçlar

c. Hissedarlar

d. Müşteriler

96. Felaket kurtarma ile ilgili eğitim neden bir DRP projesinde hayati bir bileşendir?

a. Plan onaylanabilecek

b. Kurtarma, dış kuruluşlar tarafından gerçekleştirilir

c. Sistemlere en aşina olan personel bir afet sırasında müsait olmayabilir.

d. Personel kurtarma prosedürlerine aşina olmayabilir

97. Kritik iş süreçlerinin aksama süresinin maliyetini anlamak neden önemlidir?

a. Yönetim, hafifletici kontrollerin maliyeti ve acil durum planları hakkında kararlar alabilecektir.

b. Yönetim, hangi süreçlerin en kritik olduğunu belirleyebilecek

c. Yönetim bir eğitim bütçesi oluşturabilecektir

d. Yönetim, kurtarma maliyetlerini benzer kuruluşlardakilerle karşılaştırabilecektir

98. Kurtarma Noktası Hedefinin (RPO) tanımı şöyledir:

a. Kurtarma sitesinin yeri

b. Maksimum kesinti süresi

c. Yedek verileri kurtarmak için kullanılan yöntem

d. Maksimum veri kaybı miktarı

99. Kurtarma Süresi Hedefinin (RTO) tanımı şöyledir:

a. Kurtarma sitesinin yeri

b. Maksimum kesinti süresi

c. Yedek verileri kurtarmak için kullanılan yöntem

d. Maksimum veri kaybı miktarı

100. Bir DRP proje ekibi, belirli bir uygulama için RTO'nun 180 dakikaya ayarlanacağını belirlemiştir. Bir kurtarma sistemi için hangi seçenek uygulamanın kurtarma ihtiyaçlarını en iyi şekilde karşılayacaktır?

a. Çalışırken bekleme sistemleri ve teyp kurtarma

b. Sunucu kümeleme ve veri çoğaltma

c. Açık bekleme sistemleri ve teyp kurtarma

d. Soğuk site ve teyp kurtarma

Bölüm 5

101. Şifreli metni düz metne dönüştürme süreci şu şekilde bilinir:

a. Şifre çözme

b. Şifreleme

c. Anahtar kurtarma

d. Hashing

102. Vernam şifresi hakkında aşağıdaki ifadelerden hangisi doğrudur?

a. Polifabetik bir şifredir

b. Bu bir çalışan anahtar şifresidir

c. Şifreleme anahtarı yalnızca bir mesaj için kullanılır

d. Bunun başka bir adı da tek seferlik bir karmadır.

103. Tek seferlik bir ped için minimum anahtar uzunluğu nedir?

a. 128 bit

b. 64 bit

c. 56 bit

d. Düz metin mesajının uzunluğu

104. Çok alfabeli şifre ile ilgili aşağıdaki ifadelerin tümü, HARİÇ:

a. Tek seferlik bir ped şeklidir

b. Frekans analizi saldırılarına karşı dayanıklıdır

c. Birden fazla ikame alfabesi kullanır

d. Bu bir tür ikame şifresidir

105. Çalışan anahtar şifresi şu durumlarda kullanılabilir:

a. Düz metin, şifreleme anahtarından daha uzun

b. Düz metin, şifreleme anahtarından daha kısadır

c. Düz metin akış medyasıdır

d. Düz metin hızla değişiyor

106. Modulo aritmetiğinde, A - B <0 olduğunda, o zaman:

a. 26 sonuçtan çıkarılır

b. Sonuca 100 eklenir

c. Sonuca 26 eklenir

d. Sonuca 32 eklenir

107. Bir bilgisayar kullanıcısı, bir SSL VPN aracılığıyla İnternette bir ses yayınını dinliyor. Bu durumda kullanılan şifreleme şifresi türü:

a. Blok şifresi

b. Kesintisiz şifreleme

c. Anahtar şifreleme çalıştırılıyor

d. Vernam şifresi

108. Bir elektronik kod kitabı (ECB) şifresinde, her şifreli metin bloğu:

a. Sonraki bloğu şifrelemek için kullanılır

b. Önceki bloğu şifrelemek için kullanılır

c. Sonraki bloğun şifresini çözmek için kullanılır

d. Sonraki bloğu şifrelemek için kullanılmaz

109. Bir sonraki blok için kullanılan şifrelemede her şifrelenmiş düz metin bloğundan şifreli metin çıktısının bulunduğu şifreleme modu şu şekilde bilinir:

a. Şifre geri bildirimi

b. Çıktı geri bildirimi

c. Şifre bloğu zincirleme

d. Elektronik kod kitabı

110. Genel anahtar şifrelemesi şunun başka bir adıdır: Güvenli

a. Yuva Katmanı

b. Asimetrik kriptografi

c. Simetrik anahtar şifreleme

d. Kerberos

111. Açık anahtar şifrelemesi böyle adlandırılmıştır çünkü:

a. HTTPS için dünya standardıdır

b. Tüm popüler bilgisayar işletim sistemlerinde çalışır

c. Halka açıklanabilen bir şifreleme anahtarı kullanır

d. Şifreleme algoritmaları kamu alanında bulunur

112. Bir güvenlik yöneticisi, kullanılacak bir şifreleme algoritması arıyor hassas bilgiler içeren veri dosyalarını şifrelemek. Aşağıdaki algoritmalardan hangisi DÜŞÜNÜLMEMELİDİR:

a. BALIK

b. İki balık

c. Balon balığı

d. OYUNCULAR

113. Belirli bir şifreleme algoritması, şifreleme anahtarıyla düz metni XORlayarak düz metni şifreli metne dönüştürür. Bu şu şekilde bilinir:

a. Elektronik kod kitabı

b. Şifre bloğu zincirleme

c. Blok şifresi

d. Kesintisiz şifreleme

114. Daha önce hiç iletişim kurmamış iki taraf, simetrik şifreleme anahtarı şifreleme kullanarak mesaj göndermek istemektedir. Partiler nasıl başlamalı?

a. Alıcı taraf, açık şifreleme anahtarını ileten tarafa göndermelidir.

b. Her taraf, genel şifreleme anahtarlarını değiş tokuş etmelidir.

c. Her bir taraf, şifreleme anahtarını iletişim kanalı üzerinden diğer tarafa göndermelidir.

d. Bir taraf, şifreleme anahtarını bant dışı bir iletişim kanalı aracılığıyla diğer tarafa iletmelidir.

115. Daha önce hiç iletişim kurmamış iki taraf göndermek istiyor asimetrik anahtar şifreleme kullanan mesajlar. Partiler nasıl başlamalı?

a. Alıcı taraf, kendi özel şifreleme anahtarını ileten tarafa göndermelidir.

b. İleten taraf, kendi özel şifreleme anahtarını alıcı tarafa göndermelidir.

c. Alıcı taraf, açık şifreleme anahtarını ileten tarafa göndermelidir.

d. İleten taraf, açık şifreleme anahtarını alıcı tarafa göndermelidir.

116. İki taraf, Parti A ve Parti B, kullanarak düzenli olarak mesaj alışverişinde bulunur. açık anahtarlı kriptografi. Taraflardan biri, Taraf A, özel şifreleme anahtarının tehlikeye atıldığına inanıyor. Parti B ne yapmalı?

a. Taraf A'dan yeni bir genel anahtar isteyin.

b. A Tarafından yeni bir özel anahtar talep edin.

c. A Partisine yeni bir genel anahtar gönderin.

d. A Grubuna yeni bir özel anahtar gönderin.

117. Gelişmiş Şifreleme Standardı, şifrelemenin:

a. Dijital Şifreleme Algoritması (DEA)

b. 3DES

c. Rijndael

d. Uluslararası Veri Şifreleme Algoritması (IDEA)

118. Veri Şifreleme Standardı:

a. Güvenli Yuva Katmanı (SSL) şifrelemesi tarafından kullanılır

b. Uluslararası Veri Şifreleme Algoritması (IDEA) ile değiştirildi

c. 64 bit şifreleme anahtarı kullanır

d. 56 bitlik bir şifreleme anahtarı kullanır

119. İki taraf, açık anahtar şifrelemesini kullanarak mesaj alışverişi yapıyor. Aşağıdaki ifadelerden hangisi şifrelenmiş bir mesajı iletmek için uygun prosedürü açıklamaktadır?

a. Gönderen, alıcının genel anahtarını kullanarak mesajı şifreler ve alıcı, alıcının özel anahtarını kullanarak mesajın şifresini çözer.

b. Gönderen, gönderenin genel anahtarını kullanarak mesajı şifreler ve alıcı, alıcının genel anahtarını kullanarak mesajın şifresini çözer.

c. Gönderen, gönderenin özel anahtarını kullanarak mesajı şifreler ve alıcı, alıcının özel anahtarını kullanarak mesajın şifresini çözer.

d. Gönderen, gönderenin genel anahtarını kullanarak mesajı şifreler ve alıcı, gönderenin genel anahtarını kullanarak mesajın şifresini çözer.

120. Bir akış şifresi, şifreleme ile düz metni XORing yaparak verileri şifreler anahtar. Şifreli metin nasıl tekrar düz metne dönüştürülür?

a. Şifreleme anahtarıyla XORing

b. Şifreleme anahtarının tersi ile onu XORing

c. VE şifreleme anahtarıyla birlikte

d. Şifreleme anahtarıyla NAND yapmak

121. Bir mesajı dijital olarak imzalamanın amacı aşağıdakileri sağlamaktır:

a. Gönderenin bütünlüğü

b. Mesajın gizliliği

c. Gönderenin gerçekliği

d. Gönderenin gizliliği

122. Bir mesajı dijital olarak imzalamanın amacı şunları sağlamaktır:

a. Mesajın bütünlüğü

b. Mesajın gizliliği Gönderenin

c. bütünlüğü

d. Gönderenin gizliliği

123. Diffie-Hellman anahtar değişim protokolünün amacı şudur: Simetrik bir şifreleme

a. anahtarının şifresini çözmek

b. Simetrik bir şifreleme anahtarını şifrelemek için

c. Hiçbir zaman iletişim kurmayan iki tarafın genel şifreleme anahtarları oluşturmasına izin vermek için

d. Hiç iletişim kurmayan iki tarafın gizli bir şifreleme anahtarı oluşturmasına izin vermek için

124. Bir saldırgan, kullanılan şifreleme anahtarını öğrenmeye çalışıyor.
iki taraf arasında gönderilen mesajları korumak. Saldırgan kendi mesajlarını oluşturabilir, bunları taraflardan biri tarafından şifrelenebilir ve ardından mesajının şifreli metnini inceleyebilir. Bu tür saldırı şu şekilde bilinir:

a. Yalnızca şifreli metin saldırısı

b. Şifreli metin saldırısı

c. Seçilmiş düz metin saldırısı

d. Ortadaki saldırıdaki adam

125. Paylaştıkları mesajların gizliliğini ve bütünlüğünü teyit etmek için bir araç oluşturmak isteyen iki taraf için en iyi yaklaşım hangisidir:

a. Dijital imzalar

b. Şifreleme ve dijital imzalar

c. Anahtar değişimi

d. Şifreleme

Bölüm 6

126. ABD'deki yasa kategorileri şunlardır:

a. Sivil, cezai, idari ve aile

b. Fikri, mahremiyet ve bilgisayar suçları

c. Ceza, medeni ve idari

d. Ceza, medeni ve aile

127. Ticari markalar, telif hakları ve patentler aşağıdakilerin bir parçasıdır:

a. Fikri mülkiyet hukuku

b. Sivil yasa

c. İdari hukuk

d. Özel mülkiyet hukuku

128. Bir kuruluş yeni bir yazıcı türü geliştirdi. Ne yaklaşımı organizasyon bu buluşu korumalı mı?

a. Meslek sırrı

b. Telif hakkı

c. Marka

d. Patent

129. Bir mali hizmetler kuruluşunun müşterileri hakkındaki bilgileri koruması gerekir. Bu yasalardan hangisi bu korumayı gerektirir:

a. HIPAA

b. COPPA

c. CALEA

d. GLBA

130. Bir şüpheli, ATM'den para çekme yoluyla sahiplerinden para çalmak amacıyla kredi kartı sahteciliği yapmaktadır. Bu şüpheli büyük olasılıkla hangi ABD yasalarına göre yargılanacak?

a. Bilgisayar Dolandırıcılığı ve Kötüye Kullanım Yasası

b. Cihaz Dolandırıcılığına Erişim

c. Bilgisayar Güvenliği Yasası

d. Sarbanes-Oxley Kanunu

131. Hangi ABD yasaları, kolluk kuvvetlerine telefon, e-posta, bankacılık ve diğer kayıtları arama konusunda daha fazla yetki verir?

a. Vatanseverlik Yasası

b. Hukuki Yaptırım Yasası için İletişim Yardımı

c. Federal Bilgi Güvenliği Yönetimi Yasası

d. Gramm-Leach-Bliley Yasası

132. Ödeme Kartı Sektörü Veri Güvenliği Standardı (PCI DSS), aşağıdaki durumlarda kredi kartının şifrelenmesini gerektirir:

a. Veritabanlarında depolanır, düz dosyalarda depolanır ve genel ve özel ağlar üzerinden iletilir

b. Veritabanlarında saklanır ve halka açık ağlar üzerinden iletilir

c. Veritabanlarında depolanır, düz dosyalarda depolanır ve genel ağlar üzerinden iletilir

d. Veritabanlarında saklanır ve genel ve özel ağlar üzerinden iletilir

133. Yetkisiz giriş olarak tanımlanan bir

a. güvenlik olayı

b. Hassas bilgilerin ifşa edilmesi Hassas

c. bilgilerin çalınması

d. Güvenlik politikasının ihlali

134. Kapsamlı bir güvenlik olay planının aşamaları şunlardır:

a. Beyan, triyaj, soruşturma, analiz, çevreleme, kurtarma, bilgi alma

b. Araştırma, analiz, çevreleme, kurtarma, bilgi alma Beyanı, triyaj,

c. çevreleme, kurtarma, bilgi alma

d. Beyan, triyaj, soruşturma, analiz, dokümantasyon, sınırlama, kurtarma, bilgi alma

135. Bir güvenlik yöneticisi, hassas bilgilerin şurada depolandığını keşfetti:
bir sunucunun güvenliği ihlal edildi. Organizasyon, kanunen kolluk kuvvetlerine bildirimde bulunmak zorundadır. Sunucudaki kanıtları korumak için güvenlik yöneticisi ilk önce ne yapmalıdır:

a. Sunucuya giden gücü kesin

b. Sunucuyu yedekleyin

c. Sunucuyu kapatın

d. Hata ayıklama modunu etkinleştirin

136. Bir güvenlik olayı planıyla ilgili aşağıdaki ifadelerin tümü, HARİÇ:

a. Plan yıllık olarak test edilmelidir

b. Plan yıllık olarak gözden geçirilmelidir

c. Plan yıllık olarak yayınlanmalıdır

d. Plan prosedürleri ile ilgili eğitim yıllık olarak yapılmalıdır

137. Bir güvenlik olayı sorgusunun amacı, aşağıdakilerin tümü HARİÇ:

a. Günlük dosyalarının gözden geçirilmesi

b. Teknik mimarinin gözden geçirilmesi

c. Operasyonel prosedürlerin gözden geçirilmesi

d. Teknik kontrollerin gözden geçirilmesi

138. Bir adli tıp araştırmacısı, adli tıp araştırması sırasında neden bilgisayarın çevresini incelemek ister?

a. Temizliği değerlendirin

b. Şüpheliyi sorgulayın

c. DNA kanıtı arayın

d. Çıkarılabilir medya ve belgeleri arayın

139. Adli tıp soruşturmasına konu olan bir çalışan suistimali vakası, muhtemelen bir mahkeme işlemiyle sonuçlanacaktır. Adli soruşturmaya neler dahil edilmelidir:

a. Tüm aktiviteler hakkında okunaklı notlar

b. Kolluk soruşturması

c. Tüm kanıtlar için gözetim zinciri

d. Tüm kanıtlar için çifte velayet

140. (ISC) ² etik kuralları aşağıdakilerin tümünü içerir, HARİÇ:

a. Müdürlere özenli ve yetkin hizmet sunmak

b. Toplumu ve altyapıyı koruyun

c. Onurlu, dürüst, adil, sorumlu ve yasal olarak hareket edin

d. Mesleği ilerletin ve koruyun

141. Bir güvenlik yöneticisinden, üst düzey bir yönetici tarafında çalışan davranışını araştırması istenmiştir. Soruşturma, konunun yargılamada ciddi bir gecikme yaşadığını ve davayı ihlal ettiğini göstermiştir.
kuruluşun davranış kuralları. Güvenlik yöneticisinden soruşturmanın sonuçlarını gizli tutması istendi. Güvenlik yöneticisi nasıl yanıt vermeli?

a. Soruşturmanın sonuçlarını medyaya sızdırmak

b. Soruşturmanın sonuçlarını örtbas edin

c. Soruşturmanın sonuçlarını ve sonraki adımlar için tavsiyeleri amirlerine iletin

d. Kolluk kuvvetlerine bildir

142. Bir adli tıp araştırmacısından iş istasyonunu incelemesi istendi
geçmişte yaramazlık yaptığı bilinen bir çalışan tarafından kullanılır. Bu soruşturma, daha fazla olası suistimalle ilgilidir. Araştırmacı bu yeni araştırmada hangi yaklaşımı benimsemelidir?

a. Bu çalışanın davranış geçmişine bakmaksızın bu soruşturmaya objektif bir şekilde yaklaşın

b. Bu çalışanın davranış geçmişi göz önüne alındığında, bu soruşturmaya öznel olarak yaklaşın

c. Çalışanın suçlu olduğunu varsayın ve bunu destekleyecek kanıt arayın Çalışanın masum

d. olduğunu varsayın ve bunu çürütmek için kanıt arayın

143. Bir çalışanın şirket politikasını ihlal ettiği iddiası
çocuk pornografisini bir şirketin iş istasyonuna indirmek şu sonuçlara yol açmalıdır:

a. Etkilenen müşterilerin bildirimi

b. Çalışanın feshi

c. Bir güvenlik olayının ilanı

d. Adli soruşturma ve olası disiplin cezası

144. Bir kuruluş, ilk bilgisayar güvenliği olay müdahale prosedürünü geliştirmiştir. İlk olarak ne tür bir test yapılmalıdır?

a. Paralel test

b. Simülasyon

c. İzlenecek yol

d. Belge incelemesi

145. Bir kuruluşun güvenlik olayı yönetimi stratejisi, bir olay meydana geldiğinde kullanılacak müdahale prosedürlerinden oluşur. Kuruluş başka hangi önlemleri almalıdır:

a. Yok

b. Olayların önlenmesine yardımcı olmak için proaktif prosedürler geliştirin

c. Seçilen personeli olay müdahale prosedürleri konusunda eğitin

d. Olay müdahale prosedürlerinde kolluk kuvvetleriyle ortak olun

146. Bir güvenlik olayı müdahale planındaki çevreleme adımının amacı:

a. Olayın yayılmasını önlemek için

b. Etkilenen sistemi olay öncesi durumuna kurtarmak için

c. Sistemi izole etmek için

d. Olası disiplin cezası veya kovuşturması için kanıt toplamak için

147. İstenmeyen ticari e-posta göndermeyi yasa dışı yapan ABD yasası şöyledir:

a. SPAMI DURDUR

b. DMCA

c. İstenmeyen Pornografi Saldırısını Kontrol Etme ve Pazarlama Yasası

d. Bilgisayar Güvenliği Yasası

148. ABD'deki idari kanunların amacı şudur:

a. Mahkeme salonu ve kanun uygulama prosedürlerini tanımlamak

b. Saldırı, kundakçılık, hırsızlık, hırsızlık, rüşvet, yalancı şahitlik gibi faaliyetleri tanımlamak

c. Sözleşme, haksız fiil, mülk, istihdam ve şirketler hukukunu tanımlamak için

d. ABD devlet kurumlarının işleyişini düzenlemek için

149. ABD Kodu şunları tanımlar:

a. Hem ceza hem de medeni kanunlar

b. İdari kanunlar

c. Medeni kanunlar

d. Ceza kanunları

150. Yazılı bir eseri koruyan fikri mülkiyet yasasının türü şu şekilde bilinir:

a. Telif hakkı

b. Marka

c. Patent

d. Servis işareti

Bölüm 7

151. Bir organizasyondaki bir çalışan, gerekenden daha fazla bilgiye erişim talep ediyor. Bu talep, hangi ilkeye dayanarak reddedilmelidir:

a. Görevlerinin ayrılması

b. En az ayrıcalık

c. Bilmem gerek

d. İş rotasyonu

152. Hassas bilgiler içeren kasayı iki ayrı çalışanın açması gerekmektedir. Bir çalışanın kasa kombinasyonunun bir parçası ve ikinci bir çalışanın kasa kombinasyonunun başka bir kısmı vardır. Bu düzenleme şu ilkeyi izler:

a. Bölünmüş velayet

b. Görevlerin ayrılığı

c. Bilmem gerek

d. En az ayrıcalık

153. Bir organizasyondaki bilgi güvenliği görevlisi, mümkün olan en az fonksiyona sahip roller atamaya özen göstererek, çeşitli muhasebe departmanı çalışanlarını organizasyonun finansal sistemindeki çeşitli rollere atamıştır. Roller şu ilkeye göre atanmıştır:

a. Bilmem gerek

b. Görevlerin ayrılığı

c. Bölünmüş velayet

d. En az ayrıcalık

154. Bir kuruluşun elinde, hassasiyet ve kullanım gereksinimleri bakımından değişen birçok iş kaydı türü vardır. Bu kayıtlardan herhangi birinin nasıl korunması gerektiğini tanımlayan hiçbir politika yoktur. Bu organizasyonda eksikler:

a. Saklama ve taşıma prosedürleri

b. Görevlerinin ayrılması

c. Veri sınıflandırma politikası

d. Bilgi güvenliği politikası

155. Kullanıcı erişim haklarının periyodik olarak incelenmesinin amacı şudur:

a. Çalışanların sisteme giriş yapıp yapmadığını kontrol etmek için

b. İşine son verilen çalışanlara ait aktif hesapları kontrol etmek için

c. Parola kalitesini ve son kullanma tarihini belirlemek için

d. Erişim kontrol sistemlerinin hala düzgün çalışıp çalışmadığını belirlemek için

156. Parola değişiklikleri arasında minimum gün sayısı gerektiren bir parola politikasının amacı şudur:

a. Bir şifreye karşı kaba kuvvet saldırısını önlemek için

b. İzinsiz giren bir kişinin bir şifreye karşı sözlük saldırısı yapmasını önlemek için

c. Birinin bilindik şifresine hızla geri dönmesini önlemek için

d. İkinci bir kullanıcının şifreyi değiştirmesini önlemek için

157. Beşten sonra bir hesabı kilitleyen bir şifre politikasının amacı başarısız oturum açma girişimleri:

a. İzinsiz giren bir kişinin bir şifreye karşı sözlük saldırısı yapmasını önlemek için

b. İkinci bir kullanıcının şifreyi değiştirmesini önlemek için

c. Birinin bilindik şifresine hızla geri dönmesini önlemek için

d. Diğer kişilerin hesaba giriş yapmasını önlemek için

158. Yedeklemelerin amacı aşağıdakilerin tümünü içerir, HARİÇ: Yazılım

a. arızaları

b. İnsan hatası

c. Donanım arızaları

d. Küme yük devretmeleri

159. Yedeklemelerin düzgün çalışıp çalışmadığını doğrulamanın en etkili yolu şudur:

a. Yedekleme günlüklerinde hata mesajlarının varlığının doğrulanması

b. Yedekleme günlüklerinde hata mesajlarının bulunmadığının doğrulanması

c. Verileri yedekleme ortamına yedekleme yeteneğini test etme

d. Verileri yedekleme ortamından geri yükleme yeteneğini test etme

160. Bir kuruluşun veri sınıflandırma politikası, her hassasiyet düzeyindeki veriler için işlem prosedürlerini içerir. BT departmanı, tüm verileri manyetik bant üzerine yedekler ve sonuçta tüm hassasiyet düzeylerinde veri içeren bantlar elde edilir. Bu yedekleme bantları nasıl kullanılmalı?

a. En düşük hassasiyet seviyesi prosedürlerine göre

b. En yüksek hassasiyet seviyesi prosedürlerine göre

c. En düşük ve en yüksek hassasiyet seviyeleri arasındaki prosedürlere göre

d. Veri işleme prosedürleri yedekleme medyası için geçerli değildir, sadece orijinal medya

161. Sabit disk sürücülerindeki verileri yok etmek için aşağıdaki yöntemlerin tümü HARİÇ yeterli:

a. Yeniden biçimlendirme

b. Manyetikliği giderme

c. Parçalama

d. Sondaj

162. Aşağıdakilerin tümü, verileri yedeklemek için geçerli nedenlerdir, HARİÇ: Afet

a.

b. Verileri bozan yazılım hataları

c. Çoğaltma

d. Sabotaj

163. Bir kuruluşun BT yöneticisi bir iş ilişkisi kuruyor
yedekleme medyasının depolanması için tesis dışı bir medya depolama şirketi ile. Depolama şirketinin, kuruluşun veri merkezinden 8 mil uzakta bir konumu ve 113 mil uzakta başka bir konumu vardır. Neden bir yer diğerine tercih edilmeli?

a. Hangi tesisin seçildiği fark etmez

b. Periyodik yerinde denetimleri kolaylaştırmak için daha yakın konum seçilmelidir

c. Daha hızlı iyileşmeyi kolaylaştırmak için daha yakın konum seçilmelidir

d. Bölgesel bir afetten etkilenmeyeceği için daha uzak yer seçilmelidir.

164. Bir kuruluşun BT yöneticisi işi bırakmak istiyor
Bir site dışı medya depolama şirketi ile ilişki kurabilir ve bunun yerine kuruluşun yedekleme bantlarını kuruluşun veri merkezine daha yakın olan evinde saklayın. Bu plan dikkate alınmalı mı ve neden:

a. Medya daha az fiziksel korumaya sahip olacağı için bu dikkate alınmamalıdır.

b. Paradan tasarruf edeceği için bu dikkate alınmalıdır

c. Bu, kuruluşun veri merkezine daha yakın olduğu için dikkate alınmalıdır.

d. Bu, kuruluşun veri merkezine çok yakın olduğu için seçilmemelidir.

165. Sistem yöneticilerinin eylemlerinin neden daha fazla izlenmesi gerekiyor?
diğer personelden daha yakın mı?

a. Yönetici eylemleri daha zararlı olabilir ve organizasyon üzerinde daha büyük bir etkiye sahip olabilir

b. Yöneticilerin hata yapma olasılığı daha yüksektir Yöneticilerin diğer tüm

c. kullanıcıların parolalarına erişimi vardır Yönetim arayüzlerinde daha az

d. güvenlik vardır

166. Aşağıdakilerden hangisi uzaktan erişimle ilişkili bir risk DEĞİLDİR:

a. Hassas bilgilerle ilişkili risk, kuruluşun kontrolü dışında şirkete ait olmayan bir bilgisayarda saklanır.

b. Yetersiz kötü amaçlı yazılımdan koruma korumasına sahip şirkete ait olmayan bir bilgisayar, uzaktan erişim yoluyla bir virüs bulaşmasına neden olabilir

c. Uzak bilgisayardaki anti-virüs yazılımı, virüs tanımı güncellemelerini indiremeyecek

d. Bölünmüş bir tünel kullanılırsa, uzaktaki bilgisayar saldırılara karşı daha savunmasız olabilir

167. Kuruluşun ağına uzaktan erişebilen bir iş istasyonu VPN aracılığıyla ve yerel LAN'a erişim, hepsi aynı fiziksel ağ bağlantısı üzerinden, şunları kullanıyor:

a. Bölünmüş tünelleme

b. Ağ geçitlerini ayır

c. IPsec VPN yazılımı

d. SSL VPN yazılımı

168. arasındaki fark nedir *bölünmüş tünelleme* ve *ters bölünme tünel açma:*

a. Yalnızca ters bölünmüş tünelleme bir güvenlik duvarı kullanabilir

b. Yalnızca bölünmüş tünelleme bir güvenlik duvarı kullanabilir

c. Bölünmüş tünelleme IPsec ve SSL kullanırken ters bölünmüş tünelleme L2TP kullanır

d. Bölünmüş tünellemede varsayılan ağ LAN'dır; ters bölünmüş tünellemede varsayılan ağ VPN'dir

169. Bir merkezi yönetim konsolu kullanımının birincil avantajı anti-virüs:

a. Merkezi virüs tespiti

b. Merkezi raporlama

c. Raporlama ve merkezi imza dosyası dağıtımının birleştirilmesi

d. Merkezi imza dosyası dağıtımı

170. Güçlü bir manyetik alan kullanarak manyetik ortamı silme işlemi şu şekilde bilinir:

a. Delousing

b. Manyetikliği giderme

c. Parçalama

d. Silme

171. Bir güvenlik yöneticisi, bir sistem yöneticisine sabit diskteki dosyaları temizlemesi talimatını verdi. Bu, yöneticinin şunları yapması gerektiği anlamına gelir:

a. Sabit diskte düşük seviyeli bir format gerçekleştirin

b. Sabit diskteki manyetik depolama malzemesini yeniden hizalamak için bir degausser kullanın

c. Dosyaların üzerine birden çok kez yazmak için bir araç kullanın

d. Sabit diskte yüksek seviyeli bir format gerçekleştirin

172. Bir kuruluş, operasyon departmanındaki faaliyetlerle ilgili bir dava ihbarı aldı. onunKuruluş nasıl yanıt vermelidir:

a. Bir sonraki duyuruya kadar tüm tasfiye faaliyetlerini durdurun

b. Saklama programlarını değiştirin ve en eski bilgileri temizlemeye başlayın

c. Saklama programında belirtilen zaman çizelgelerinden daha eski tüm bilgileri temizleyin

d. Tüm tasfiye faaliyetlerini gerçekleştirmek için dışarıdan bir kuruluş kiralayın

173. Bir kuruluş, masaüstünde birkaç virüs bulaşması yaşadı iş istasyonları. Aşağıdaki çözümlerden hangisi virüs enfeksiyonlarını azaltmada etkili OLMAZ?

a. Bir anti-virüs ağ geçidi web proxy sunucusu kurun

b. E-posta sunucularına anti-virüs kurun

c. Anti-virüs merkezi yönetim konsolunu kurun

d. Web sunucularına anti-virüs kurun

174. Bir örgüt, hukuk davasına taraf oldu. Organizasyonun, elektronik kayıtlarını belirli memorandalar için araştırması gerekmektedir. Bu süreç şu şekilde bilinir:

a. Mahkeme celbi

b. Arama ve el koyma

c. Keşif

d. Elektronik keşif

175. Bir kuruluşun kritik uygulamasının, her ay sadece birkaç dakikalık kesinti süresine izin verilerek, sürekli olarak erişilebilir olması gerekir. Kuruluş, bu düzeyde kullanılabilirliği sağlamak için hangi önlemleri uygulamalıdır?

a. Sunucu kümeleme

b. Sunucu kümeleme ve veri çoğaltma

c. Sıcak bekleme sitesi

d. Veri kopyalama

Bölüm 8

176. Bir iş tesisine fiziksel erişimi kontrol etmek için anahtar kartların kullanımı aşağıdaki şekillerde olabilir:

a. Hem önleyici hem de idari kontrol

b. Dedektif kontrolü

c. Hem önleyici hem de dedektif kontrol

d. Önleyici kontrol

177. Bir güvenlik yöneticisi, kayıp anahtar kartlarının bir tesise girmek için bir davetsiz misafir tarafından kullanılabileceğinden endişe duymaktadır. Bunu önlemek için hangi önlem kullanılabilir?

a. Kart okuyucu istasyonlarında PIN pedlerini uygulayın

b. Kart okuyucu istasyonlarında video gözetimi uygulayın

c. Kart okuyucu istasyonlarında insan tuzakları uygulayın

d. Kart okuyucu istasyonlarında RFID sensörleri uygulayın

178. Bina giriş kontrolü için uygun yaygın biyometrik çözümler şunları içerir:

a. Ses baskısı ve yürüyüş

b. Retina tarama ve el baskısı

c. Ses baskısı ve DNA

d. Parmak izi ve el izi

179. Bir seferde yalnızca bir kişinin geçebileceği bir bina erişim mekanizmasına a:

a. Giriş tuzağı

b. Adım tuzağı

c. Mantrap

d. Passtrap

180. Bir kuruluşun, en kararlı davetsiz misafirleri uzak tutmak için bir duvar veya çit yapması gerekir. Organizasyon ne inşa etmelidir?

a. Sekiz fit yüksekliğinde bir çit veya duvar

b. Üç ayaklı dikenli tel ile sekiz fit yüksekliğinde bir çit veya duvar

c. On iki fit yüksekliğinde bir çit veya duvar

d. Tek telli dikenli tel ile altı fit yüksekliğinde bir çit veya duvar

181. İzinsiz girenleri tespit etmek için çitler ve duvarlarla birlikte hangi kontroller kullanılabilir?

a. Video izleme

b. Hareket dedektörleri

c. Video izleme ve hareket dedektörleri

d. Görünür bildirimler

182. Gizli video gözetimi yapmak isteyen bir kuruluş şunları kullanmayı düşünmelidir:

a. Gizli video kameralar

b. Pan / tilt / zoom kameraları

c. Gece görüş kameraları

d. Hava koşullarına dayanıklı kameralar

183. Aşağıdakilerden hangisi caydırıcı bir kontrol DEĞİLDİR:

a. Video gözetimini gösteren monitörler

b. Bekçi köpekleri

c. Gözetim bildirimleri

d. Mantrap

184. Kritik alanları aydınlatmak için gereken minimum aydınlatma miktarı nedir?

a. 12 fit yükseklikte 6 fitlik mumlar

b. 12 fit yükseklikte 2 fitlik mumlar

c. 8 fit yükseklikte 4 fitlik mumlar

d. 8 fit yükseklikte 2 fitlik mumlar

185. Bir güvenlik yöneticisi, araçların geçişini engelleyecek, ancak yaya trafiğine serbestçe izin verecek bariyerler uygulamak ister. Uygulanması gereken kontrol şudur:

a. Turnikeler

b. Bollards

c. Çarpışma kapıları

d. Düşük duvarlar

186. Güvenli bir tesisin gelen araç trafiğini kontrol etmesi ve belirli saldırıları durdurabilmesi gerekir. Hangi kontrol uygulanmalıdır:

a. Çarpışma kapısı

b. Muhafız karakolu

c. Turnike

d. Bollards

187. Güvenliğe önem veren bir kuruluş, iş ofisini paylaşılan bir kiracı binasına taşıyor. Personel girişi nasıl kontrol edilmelidir?

a. Tüm kiracılar tarafından ortaklaşa çalıştırılan tek bir anahtar kart sistemi

b. Her kiracı tarafından çalıştırılan ayrı anahtar kart sistemleri

c. Binaya kimlerin girebileceğini kontrol etmek için güvenlik görevlileri

d. Binaya kimin girdiğini izlemek için video gözetimi

188. Yanıcı sıvılara karşı hangi tip yangın söndürücü etkilidir:

a. C sınıfı

b. K sınıfı

c. A sınıfı

d. B sınıfı

189. Görünmeden önce dumanı algılamak için tasarlanmış duman dedektörü türü:

a. İyonlaşma

b. Optik

c. Ultraviyole

d. Radyoaktif

190. Yerel yangın yasalarının izin vermesi koşuluyla, bilgisayar odaları için en çok hangi tip yangın sprinkler sistemi tercih edilir?

a. Ön eylem sistemi

b. Baskın sistemi

c. Islak boru sistemi

d. Köpük su sistemi

191. Gazlı yangın söndürme sisteminin avantajı şudur:

a. Odadaki oksijeni değiştirerek çalışır

b. İnsanlar için tehlikelidir

c. Bilgi işlem ekipmanına zarar vermez

d. Yağmurlama sistemlerinden daha ucuzdur

192. Bir bilgi işlem tesisinde aşırı nem riskleri aşağıdakilerin tümünü içerir, HARİÇ:

a. Statik elektrik

b. Aşınma

c. Yoğunlaşma

d. Kısa devreler

193. Kesintiler, kesintiler, dalgalanmalar ve gürültünün tümü şu yöntemlerle giderilebilir:

a. Hat düzeltici

b. Güç Dağıtım Birimi (PDU)

c. Çift güç kaynakları

d. UPS ve elektrik jeneratörü

194. Bir bilgi işlem tesisi sık sık kesinti yaşar, ancak çok az kesinti yaşar. Bu durumu hafifletmek için neler uygulanmalıdır:

a. Hat düzeltici

b. Güç Koşullandırma Birimi (PDU)

c. Kesintisiz Güç Kaynağı (UPS)

d. Elektrik jeneratörü

195. "N + 1" terimi şu anlama gelir:

a. Mevcut elektrik güç kaynağı, mevcut talebin en az iki katıdır

b. Birden çok bileşen (N) en az bir (+1) bağımsız yedekleme bileşenine sahiptir

c. Başka bir ünitede arıza veya planlı bakım durumunda en az bir (+1) yedek HVAC ünitesi vardır

d. Her sunucu ve ağ cihazı çift güç kaynağı kullanır

196. Bir kuruluş, sık sık güç deneyimleyen bir bölgede bulunur elektrik kesintileri. Bu durumda bir elektrik jeneratörünün etkisi ne olur?

a. Organizasyon sürekli bir elektrik gücüne sahip olacak.

b. Kuruluşun en az iki yakıt tedarikçisiyle yakıt tedarik sözleşmeleri yapması gerekecektir.

c. Elektrik şebekesi kesintileri, kuruluş için kısa elektrik kesintilerine neden olacaktır.

d. Bu durumda bir elektrik jeneratörü yardımcı olmayacaktır.

197. Elektrik jeneratörleri hakkında aşağıdaki ifadelerden hangisi DOĞRUDUR?

a. Jeneratörler, elektrik gücü sağlamadan önce bir ila üç dakikalık başlatma süresine ihtiyaç duyar

b. Jeneratörler, Kesintisiz Güç Kaynağı (UPS) gerektirir

c. Jeneratörler başlatma süresi gerektirmez, ancak acil durum elektrik gücünü talep üzerine anında sağlar

d. Yakıt ikmali için jeneratörlerin kapatılması gerekir

198. Bir yangın söndürücünün amacı:

a. Kazara meydana gelen yangınlarla mücadele için kullanılan birincil cihaz

b. İtfaiye gelene kadar tüm yangınlarla mücadele etmek için birincil cihaz Tüm yangınlarla mücadele

c. etmek için kullanılan birincil cihaz

d. Küçük yangınlarla savaşmak için kullanılan birincil cihaz

199. Ekipmana yönelik tehditleri tespit etmeye yönelik kontroller şunları içerir:

a. Sıcaklık sensörleri, nem sensörleri ve su dedektörleri Sıcaklık

b. sensörleri, nem sensörleri ve duman dedektörleri

c. Sıcaklık sensörleri, nem sensörleri, su dedektörleri, gaz dedektörleri ve duman dedektörleri

d. Sıcaklık sensörleri, nem sensörleri, su dedektörleri ve duman dedektörleri

200. "Güvenli konumlandırmanın" amacı:

a. Bir sitenin, devam eden iş operasyonlarını tehdit edebilecek doğal tehlikelerden makul ölçüde arınmış olmasını sağlamak için

b. Bir sitenin devam eden iş operasyonlarını tehdit edebilecek tehlikelerden makul ölçüde arınmış olmasını sağlamak için

c. Bir sitenin devam eden iş operasyonlarını tehdit edebilecek tüm tehlikelerden arınmış olmasını sağlamak için

d. Bir sitenin, devam eden iş operasyonlarını tehdit edebilecek insan kaynaklı tüm tehlikelerden arınmış olmasını sağlamak için

9. Bölüm

201. Bir dosya sunucusundaki dosya ve dizinlerin sahipleri, hangi personelin bu dosyalara ve dizinlere erişebileceğini kontrol edebilir. Buna en çok benzeyen erişim kontrol modeli:

a. Rol tabanlı erişim kontrolü (RBAC)

b. Zorunlu erişim kontrolü (MAC)

c. İsteğe bağlı erişim denetimi (DAC)

d. Çok düzeyli erişim

202. Bir kaynak sunucusu, bir erişim kontrol sistemi içerir. Bir kullanıcı bir nesneye erişim istediğinde, sistem nesnenin izin ayarlarını ve kullanıcı için izin ayarlarını inceler ve ardından kullanıcının nesneye erişip erişemeyeceğine karar verir. Buna en çok benzeyen erişim kontrol modeli:

a. Zorunlu erişim kontrolü (MAC)

b. İsteğe bağlı erişim denetimi (DAC)

c. Girişimsiz

d. Rol tabanlı erişim kontrolü (RBAC)

203. Bir güvenlik yöneticisi, bir uygulamada kaynak izinlerini ayarlıyor. Güvenlik yöneticisi, erişim izinleri içeren nesneler oluşturabileceğini ve ardından bu nesnelere bireysel kullanıcılar atayabileceğini keşfetti. Buna en çok benzeyen erişim kontrol modeli:

a. Erişim matrisi

b. Zorunlu erişim kontrolü (MAC)

c. İsteğe bağlı erişim denetimi (DAC)

d. Rol tabanlı erişim kontrolü (RBAC)

204. Bir bilgi sistemi, hem kaynaklar hem de kullanıcılar için uygulanan çok sayıda güvenlik düzeyine sahiptir. Bu sistemde, bir kullanıcı seviyesinin altındaki kaynaklara erişemez ve bir kullanıcı seviyesinin üzerinde kaynaklar oluşturamaz. Buna en çok benzeyen erişim kontrol modeli:

a. Erişim matrisi

b. Clark-Wilson

c. Biba

d. Bell-LaPadula

205. Bir güvenlik analistinin "Turuncu Kitap" adında bir sistem değerlendirme kriterleri kılavuzu vardır. Bu şunun bir parçasıdır:

a. Ortak Kriterler

b. Güvenilir Bilgisayar Güvenliği Değerlendirme Kriterleri (TCSEC)

c. Bilgi Teknolojisi Güvenliği Değerlendirme Kriterleri (ITSEC) ISO 15408

d.

206. Ortak Kriterler, hangi değerlendirme çerçevelerinin yerine geçer: Ne TCSEC ne

a. de ITSEC

b. ITSEC

c. TCSEC ve ITSEC

d. TCSEC

207. TCSEC sistem değerlendirme kriterleri şunları ele almak için kullanılır:

a. Bilginin gizliliği

b. Önleyici ve dedektif kontroller Sızma

c. testi

d. Saldırı önleme sistemleri

208. TCSEC sistem değerlendirme kriterleri, sistemlerin değerlendirilmesi için kullanılır.
ne tür:

a. E-Ticaret

b. Kamu hizmetleri

c. Bankacılık

d. Askeri

209. Bir güvenlik yöneticisi, kuruluşundaki güvenlik süreçlerinin olgunluğunu objektif olarak ölçmek ister. Bu değerlendirme için hangi model kullanılmalıdır?

a. SSE-CMM

b. SEI-CMM

c. Ortak Kriterler

d. TCSEC

210. Yazılım Mühendisliği Enstitüsü Yetenek Olgunluk Modeli Entegrasyonunun (SEI CMMI) amacı nedir?

a. Bir kuruluşun uygulama programlarının bütünlüğünün nesnel değerlendirmesi

b. Bir kuruluşun sistem mühendisliği süreçlerinin nesnel değerlendirmesi

c. Bir kuruluşun iş süreçlerinin nesnel değerlendirmesi

d. Bir kuruluşun sistem mühendisliği süreçlerinin öznel değerlendirmesi

211. Bir güvenlik görevlisi, yeni bir bilgi sisteminin kullanılmadan önce onaylanması gerektiğini beyan etti. Bunun anlamı:

a. Sistem, belirlenmiş değerlendirme kriterlerine göre değerlendirilmelidir.

b. Sistemin kullanılabilmesi için resmi bir yönetim kararı gereklidir

c. Sisteme karşı sızma testleri yapılmalıdır Sisteme karşı bir kod

d. incelemesi yapılmalıdır

212. Bir başvuru, belirlenmiş değerlendirme kriterlerine göre onaylanmıştır. Bunun anlamı:

a. Bir kod incelemesi yapıldı

b. Uygulama artık kullanılabilir

c. Kullanılmadan önce resmi yönetim onayı gereklidir

d. Uygulama zaten kullanılıyor

213. DoD Bilgi Güvencesi Belgelendirme ve Akreditasyon Süreci (DIACAP):

a. Ortak Kriterlerin yerini almıştır

b. Tüm ABD federal bilgi sistemlerinin onaylandığı ve akredite edildiği süreç

c. Yerini DITSCAP (Savunma Bakanlığı Bilgi Teknolojileri Güvenlik Sertifikasyonu ve Akreditasyon Süreci) almıştır.

d. İşlem ABD askeri bilgi sistemlerini onaylamak ve akredite etmek için kullanılıyor mu

214. Program komutlarının yürütüldüğü bilgisayardaki bileşen denir:

a. İşlemci

b. Otobüs

c. Ön taraf veriyolu

d. Firmware

215. CPU'nun Program Sayacının amacı:

a. Hafızadaki hangi talimatın şu anda üzerinde çalışıldığını takip etmek için

b. Bireysel bir programda CPU'nun tükettiği komut döngüsü sayısını takip etmek için

c. Bir programın başlangıç adresini takip etmek için CPU'nun

d. mikro kodunun sürümünü izlemek için

216. Bir CPU getirme işleminin amacı: Hafızadan

a. veri almak için

b. Hafızadan bir talimat almak için

c. Sabit disk sürücüsünden veri almak için Program

d. sayacından veri almak için

217. Uzun süreli depolama için kullanılan bir bilgisayardaki bileşene şu ad verilir:

a. İkincil depolama

b. Ana Depo

c. Sanal bellek

d. Dosya sistemi

218. Bir kaynak kodu incelemesi, şu talimatların varlığını ortaya çıkardı: kullanıcının güvenlik kontrollerini atlamasına izin verin. Kod incelemesinde ne keşfedildi?

a. Özellik

b. Bot

c. Mantık bombası

d. Arka kapı

219. Bir güvenlik yöneticisinin, işletim sistemi dosyalarının ne zaman değiştiğini düzenli olarak belirleyebilmesi gerekir. Bu görev için ne tür bir araca ihtiyaç var?

a. Olay günlüğü

b. İzinsiz giriş tespit aracı

c. Dosya sistemi bütünlüğü izleme aracı

d. Günlük analiz aracı

220. İki sistem arasında gizli bir iletişim aracı keşfedilmiştir. Bu şu şekilde bilinir:

a. Yan kanal

b. Gizli kanal

c. Steganografi

d. Bot

221. Süreç yönetimi, kaynak yönetimi, erişim yönetimi ve olay yönetimi aşağıdakilerin örnekleridir:

a. Güvenlik süreçleri

b. Bir veritabanı yönetim sisteminin işlevleri

c. Bir işletim sisteminin işlevleri

d. İşletim sistemi türleri

222. Bir işletim sisteminin en içteki kısmı şu şekilde bilinir:

a. Çekirdek

b. Çekirdek

c. Yüzük 0

d. İşlem 0

223. Bir güvenlik yöneticisi, kuruluşu tarafından satın alınan tüm yeni dizüstü bilgisayarların bir güvenlik şifreleme işlemcisi içermesini ister. Hangi donanım gerekli olmalıdır?

a. Kayan nokta yardımcı işlemci

b. Akıllı kart okuyucu

c. parmak izi okuyucu

d. Güvenilir PlatformModule (TPM)

224. Firmware bir bilgisayar sisteminde esas olarak nerede depolanır?

a. Güvenilir Platform Modülü

b. Sadece hafızayı oku

c. Ana önyükleme kaydı

d. Dosya sistemi

225. Windows işletim sistemini çalıştıran bir bilgisayarın, etkin işlemler için kullanılabilir fiziksel belleği neredeyse tükenmiştir. Mevcut tüm belleği tüketmekten kaçınmak için, işletim sistemi ne yapmaya başlamalı?

a. Takas

b. Çağrı

c. Eski süreçleri öldürmek

d. Çöp toplayıcıyı çalıştırma

Bölüm 10

226. Telekomünikasyon devrelerini inceleyen bir ağ mühendisi, DS-1 olarak etiketlenmiş bir devre buldu. Bu devreden beklenebilecek maksimum verim nedir?

a. Yaklaşık 7.000 bin karakter / sn

b. Yaklaşık 56k bit / sn

c. Yaklaşık 170 bin karakter / sn

d. Yaklaşık 1.544 milyon bit / sn

227. ATM ağlarındaki paketlerin boyutu:

a. 53 bayt

b. 1500 bayt

c. 1544 bayt

d. 64 ila 1500 bayt arasında değişken

228. Dijital abone hattı (DSL) hizmeti:

a. Mevcut kablo hizmetini kullanır ve farklı bir frekansta iletişim kurar

b. ISDN tarafından değiştirildi

c. Uydu iletişimi yerini aldı

d. Mevcut telefon hizmetlerini kullanır ve farklı bir frekansta iletişim kurar

229. Bir BT yöneticisi, ses ve veri iletişimi için birkaç şubeyi genel merkez ofisine bağlamak ister. BT yöneticisi hangi paket anahtarlamalı hizmeti dikkate almalıdır?

a. ATM

b. DSL

c. MPLS

d. Çerçeve Rölesi

230. Bir bina tesisleri yöneticisi, organizasyon için yeni bir ofis binasının inşasını denetler. Ses ve veri iletişimi için ne tür kablolama kullanılmalıdır:

a. 10BASE2 ince ağ

b. Kategori 6 bükülü çift

c. Kategori 5e çift bükümlü

d. 10BASE5 kalın ağ

231. Ethernet MAC adresleri hakkında aşağıdaki ifadelerden hangisi DOĞRUDUR:

a. MAC adresi, DHCP protokolü kullanılarak atanır

b. İlk 3 bit, cihazın üreticisini belirtir

c. İlk 3 bayt, cihazın üreticisini belirtir

d. Son 3 bayt, cihazın üreticisini belirtir

232. Bir sistem mühendisi, merkezi bir bilgisayar ve bağlı çevre birimlerinden oluşan bir sistem tasarlamaktadır. En hızlı işlem hacmi için, çevresel cihazlarla iletişim için aşağıdaki teknolojilerden hangisi kullanılmalıdır:

a. USB 2.0

b. Firewire 400

c. USB 1.1

d. IDE

233. Her istasyona giden kablolara sahip merkezi bir Ethernet anahtarından oluşan bir Ethernet ağı en iyi şu şekilde tanımlanır:

a. Mantıksal ve fiziksel yıldız

b. Mantıksal halka ve fiziksel yıldız

c. Mantıksal yıldız ve fiziksel veri yolu

d. Mantıksal veri yolu ve fiziksel yıldız

234. Bluetooth için pratik aralık:

a. 100 m

b. 300 m

c. 30 dk.

d. 10 dk.

235. "Lütfen Steve'in evcil timsahına dokunmayın":

a. TCP / IP ağındaki hizmet türlerinin adları için bir bellek yardımı

b. OSI ağ modelindeki katmanların adları için bir bellek yardımı

c. TCP / IP ağ modelindeki katmanların adları için bir bellek yardımı

d. Bir Ethernet ağındaki adres türlerinin adları için bir bellek yardımı

236. Bir kuruluş mevcut bir ofis binasını işgal etmek üzere. ağ yöneticisi tüm ağ kablolamasını inceledi ve çoğunun "Kategori 3" olarak etiketlendiğini gözlemledi. Bu kablolamada kullanılabilecek en hızlı ağ teknolojisi nedir?

a. 10 Mbit / sn Ethernet

b. 100 Mbit / sn Ethernet

c. 1000Mbit / s Ethernet

d. 10 Gbit / sn Ethernet

237. OSI ağ modeliyle ilgili aşağıdaki ifadelerin tümü, HARİÇ:

a. OSI modelinin tüm bileşenlerini içeren hiçbir ticari ağ ürünü inşa edilmemiştir.

b. OSI ağ modeli, iletişim paketleri oluşturmak için kapsüllemeyi kullanır

c. TCP / IP, OSI ağ modelinin bir uygulamasıdır

d. OSI ağ modeli, bir ağ protokol yığını modelidir

238. TCP / IP bağlantı katmanı teknolojilerinin örnekleri şunları içerir: FTP,

a. TELNET, DNS, HTTP, SMTP

b. IP, IPsec

c. TCP, UDP, ICMP

d. Ethernet, ATM, Çerçeve Geçişi, Wi-Fi

239. Bir TCP / IP ağında, bir istasyonun IP adresi 10.0.25.200'dür, alt ağ maske 255.255.252.0 ve varsayılan ağ geçidi 10.0.25.1'dir. İstasyon, IP adresi 10.0.24.10 olan başka bir istasyona nasıl paket gönderecek?

a. Paketi doğrudan istasyona gönderecek

b. Paketi 10.0.25.1'deki varsayılan ağ geçidine gönderecektir.

c. Başka bir varsayılan ağ geçidinin IP adresini bulmak için bir Proxy ARP paketi gönderecektir.

d. İstasyona paket gönderemez

240. B Sınıfı ağda kaç tane C Sınıfı ağ oluşturulabilir:

a. 254

b. 1.024

c. 16.535

d. 16.534

241. OSI modelindeki katmanlar şunlardır:

a. Bağlantı, internet aktarımı, oturum, uygulama bağlantısı,

b. internet, ulaşım, uygulama

c. Fiziksel, veri bağlantısı, ağ, taşıma, oturum, sunum, uygulama

d. Fiziksel, ağ aktarımı, oturum, uygulama

242. Bir bilgisayar yeniden başlatıldı. Bir uygulama programı başladı ve uygulama programının 10.14.250.200 IP adresindeki bir sunucuya bir FTP paketi göndermesi gerekiyor. Bunu gerçekleştirmek için bilgisayarın ağa göndereceği ilk paket nedir:

a. ARP

b. Kim

c. FTP

d. Rlogin

243. İki bilgisayar bir UDP bağlantı noktası üzerinden bir geniş alan ağında iletişim kuruyor. Bir bilgisayar, büyük bir dosyanın içeriğini diğer bilgisayara gönderiyor. Ağ tıkanıklığı bazı paketlerin gecikmesine neden oldu. TCP / IP ağ sürücüleri paket gecikmesi hakkında ne yapacak?

a. Alıcı bilgisayar, dosya aktarımının yeniden başlatılmasını isteyecektir.

b. Ağ sürücüleri paketleri uygun sıraya göre toplayacaktır.

c. Alıcı bilgisayar, gönderen bilgisayardan geciken paketleri yeniden iletmesini isteyecektir.

d. Hiçbir şey değil

244. Ağdaki bir istasyon, yüzlerce SYN paketini bir hedef bilgisayar. Gönderen bilgisayar ne yapıyor?

a. Büyük bir dosyanın içeriğini hedef bilgisayara gönderme

b. Hedef bilgisayarla bir TCP bağlantısı kurmaya çalışılıyor

c. Hedef bilgisayara SYN taşması ile saldırmak

d. Akan ses veya videoyu hedef bilgisayara iletme

245. NTP protokolünün amacı: Bir dosyanın

a. içeriğini aktarmak

b. Bilgisayar saatlerinin bir referans saate senkronizasyonu

c. Ağ üzerinden IP üzerinden Ses Paylaşımı dosya sistemleri için

d. kullanılan bir sinyal protokolü

246. Bir sistem mühendisi, bir web sunucusunun yalnızca 56-SSL bağlantılarını desteklediğini bit keşfetti. Sistem mühendisi bundan ne çıkarabilir?

a. Bu sunucuyla web iletişimi son derece güvenlidir

b. Sunucu, uzaktan yönetimi desteklemiyor

c. Bu sunucuyla yapılan web iletişimleri güvenli değildir

d. Sunucu, Windows işletim sistemini çalıştırıyor

247. Bir ağ yöneticisi, merkezi kimlik doğrulama yoluyla organizasyondaki tüm ağ cihazlarının yönetimini basitleştirmek ister. Ağ yöneticisi aşağıdaki kullanılabilir kimlik doğrulama protokollerinden hangisini seçmelidir:

a. YARIÇAP

b. TACACS

c. OSPF

d. IPsec

248. Durum bilgisi içeren paket filtreleme güvenlik duvarı bir web sunucusunu korur. Aşağıdakilerden hangisi doğrudur:

a. Güvenlik duvarı tüm kullanıcıların kimliğini web sunucusunda doğrulayacaktır

b. Güvenlik duvarı uygulama düzeyindeki saldırıları algılar ancak engellemez

c. Güvenlik duvarı, uygulama düzeyinde saldırıları engelleyecektir

d. Güvenlik duvarı, uygulama düzeyindeki saldırıları engellemeyecektir

249. Birisi bir ağın yayın adresine ICMP yankı istekleri gönderiyor. Bu kişi ne yapıyor?

a. Varsayılan ağ geçidine ping atma

b. Yönlendiriciye ping atma

c. Ping of Death saldırısı gerçekleştirmek

d. Şirin saldırısı yapmak

250. TCP protokolü hakkında aşağıdaki ifadelerin tümü, HARİÇ:

a. Doğru teslimat sırası garanti edilir

b. Bağlantısız

c. Bağlantı yönelimli

d. Eksik paketler yeniden iletilecek