CHAPTER 8

# TRUE/FALSE

**1)В допълнение към електронната поща, мигновените съобщения и споделянето на файлове чрез P2P също могат да представляват заплаха за сигурността на компютърните системи и мрежи.**

Отговор: TRUE

**2) Компютрите, които използват кабелни модеми за връзка с интернет, са по-отворени за проникване, отколкото тези, които се свързват чрез dial-up.**

Отговор: TRUE

**3) Безжичните мрежи са уязвими за проникване, тъй като радиочестотните ленти са лесни за сканиране**.

Отговор: TRUE

**4) Обхватът на Wi-Fi мрежите може да се увеличи до две мили чрез използване на външни антени.**

Отговор: FALSE

**5) Спецификацията WEP изисква точката за достъп и нейните потребители да споделят една и съща 40-битова криптирана парола**.

Отговор: TRUE

**6) Вирусите могат да се разпространяват чрез електронна поща.**

Отговор: TRUE

**7) Компютърните червеи се разпространяват много по-бързо от компютърните вируси.**

Отговор: TRUE

**8) Една от формите на подправяне включва фалшифициране на обратния адрес на електронно съобщение, така че съобщението да изглежда, че идва от някой друг, а не от изпращача.**

Отговор: TRUE

**9) Снайферите дават възможност на хакерите да крадат защитена информация от всяка точка на мрежата, включително електронни съобщения, фирмени файлове и поверителни доклади.**

Отговор: TRUE

**10) DoS атаките се използват за унищожаване на информация и за достъп до ограничени области на информационната система на компанията.**

Отговор: FALSE

**11) DoS атаките са един от най-увреждащите икономически видове компютърни престъпления.**

Отговор: TRUE

**12) Нулеви дефекти не могат да бъдат постигнати в по-големи софтуерни програми, тъй като пълното тестване на програми, които съдържат хиляди възможности за избор и милиони пътища, би отнело хиляди години.**

Отговор: TRUE

**13) Политиката за приемливо използване определя приемливото ниво на достъп до информационните активи за различните потребители.**

Отговор: FALSE

**14) Биометричната автентификация е използването на физически характеристики, като например изображения на ретината, за осигуряване на идентификация.**

Отговор: TRUE

**15) Филтрирането на пакети улавя повечето видове мрежови атаки.**

Отговор: FALSE

**16) NAT прикрива IP адресите на вътрешните хост компютри на организацията, за да възпре програмите за разузнаване.**

Отговор: TRUE

**17) SSL е протокол, който се използва за установяване на сигурна връзка между два компютъра**.

Отговор: TRUE

**18) Криптирането с публичен ключ използва два ключа.**

Отговор: TRUE

**19) Изчислителната техника с висока степен на достъпност се нарича още толерантност към грешки**.

Отговор: FALSE

**20) Както софтуерните метрики, така и софтуерното тестване са техники, използвани за подобряване на качеството на софтуера.**

Отговор: TRUE

# ИЗБИРАЕМИ

**21) \_\_\_\_\_\_\_\_ се отнася до политиките, процедурите и техническите мерки, използвани за предотвратяване на неоторизиран достъп, промяна, кражба или физическа повреда на информационните системи.**

А) „сигурност „

Б) “контрол “

В) „сравнителен анализ“ (benchmarking)

Г) „Алгоритми “

Отговор: A

**22) \_\_\_\_\_\_\_\_ се отнася до всички методи, политики и организационни процедури, които гарантират безопасността на активите на организацията, точността и надеждността на счетоводните й документи и оперативното спазване на стандартите за управление.**

А) „Наследствени системи „

Б) “Стандарти за SSID “

В) „Уязвимости „

Г) “Контроли “

Отговор: Г

**23) Кое от изброените не представлява заплаха за сигурността на безжичните мрежи?**

А) излъчвани SSID

Б) възможност за сканиране на радиочестотните ленти

В) атаки с инжектиране на SQL

Г) географски обхват на безжичните сигнали

Отговор: В

**24) Електронните данни са по-податливи на унищожаване, измами, грешки и злоупотреби, тъй като информационните системи концентрират данните в компютърни файлове, които**

А) обикновено са обвързани с наследени системи, които са трудно достъпни и трудно се коригират в случай на грешка.

Б) не са сигурни, защото технологията за тяхното осигуряване не е съществувала по времето, когато файловете са били създадени.

В) имат потенциал да бъдат достъпни от голям брой хора и от групи извън организацията.

Г) са често достъпни в интернет.

Отговор: В

**25) Неоторизираният достъп е предизвикателство за сигурността, което е най-вероятно да възникне в коя от следните точки на корпоративната мрежа?**

А) клиентски компютър

Б) комуникационни линии

В) корпоративен сървър

Г) вътрешна корпоративна бекграунд система

Отговор: A

**26) Проникването е предизвикателство за сигурността, което е най-вероятно да се появи в коя от следните точки на корпоративната мрежа?**

А) клиентски компютър

Б) комуникационни линии

В) корпоративни сървъри

Г) вътрешна корпоративна система

Отговор: Б

**27) Въвеждането на данни в лошо програмиран уеб формуляр с цел да се наруши работата на системите и мрежите на дадена компания се нарича**

А) троянски кон.

Б) атака с инжектиране на SQL.

В) регистриране на ключове.

Г) DDoS атака.

Отговор: Б

**28) Интернет създава специфични проблеми в областта на сигурността, защото**

А) е проектиран така, че да бъде лесно достъпен.

Б) данните в интернет не се пренасят по защитени линии.

В) стандартите на интернет са универсални.

Г) той се променя толкова бързо.

Отговор: A

**29) Кое от следните твърдения за сигурността в интернет не е вярно?**

А) Използването на P2P мрежи може да изложи корпоративен компютър на външни лица.

Б) Корпоративна мрежа без достъп до интернет е по-сигурна от тази, която осигурява достъп.

В) VoIP е по-сигурна от комутируемата гласова мрежа.

Г) Незабавните съобщения могат да осигурят на хакери достъп до иначе сигурна мрежа.

Отговор: В

**30) Независима компютърна програма, която се копира от един компютър на друг по мрежата, се нарича**

А) червей

Б) троянски кон

В) бъг

Г) вредител

Отговор: A

**31) Търговец кликва многократно върху онлайн рекламите на конкурент, за да увеличи разходите за реклама на конкурента. Това е пример за:**

А) фишинг.

Б) фарминг.

В) споофинг.

Г) измама с кликване (click fraud)

Отговор: Г

**32) През 2004 г. потребителите на ICQ са подмамени от търговско съобщение от предполагаем доставчик на антивирусни програми. На сайта на доставчика на машината на потребителя беше изтеглена малка програма, наречена Mitglieder. Програмата позволяваше на външни лица да проникнат в машината на потребителя. Какъв тип зловреден софтуер е пример за това?**

А) троянски кон

Б) вирус

В) червей

Г) шпионски софтуер

Отговор: A

**33) Пренасочването на уеб връзка към друг адрес е форма на**

A) шпиониране.

Б) подправяне (spoofing)

В) шпиониране.

Г) водене на война.

Отговор: Б

**34) Кийлогърът е вид**

А) червей.

Б) троянски кон.

В) вирус.

Г) шпионски софтуер.

Отговор: Г

**35) Хакерите създават ботнет, като**

A) заразяват ботове за уеб търсене със зловреден софтуер.

Б) използват ботове за уеб търсене, за да заразяват други компютри.

В) карат чужди компютри да се превърнат в „зомбита“, следващи главния компютър.

Г) заразяват корпоративни сървъри със „зомбита“ - троянски коне, които позволяват незабелязан достъп през задна врата.

Отговор: В

**36) Използването на многобройни компютри за заливане и претоварване на мрежата от многобройни стартови точки се нарича атака на \_\_\_\_\_\_\_\_.**

A) DDoS B) DoS C) SQL injection D) phishing

Отговор: A

**37) Кое от изброените не е пример за компютър, използван като цел на престъпление?**

А) съзнателен достъп до защитен компютър с цел извършване на измама

Б) достъп до компютърна система без разрешение

В) незаконен достъп до съхранена електронна комуникация

Г) заплаха за причиняване на вреда на защитен компютър

Отговор: В

**38) Кое от изброените не е пример за компютър, използван като инструмент на престъпление?**

А) кражба на търговска тайна

Б) умишлен опит за прихващане на електронна комуникация

В) неразрешено копиране на софтуер

Г) нарушаване на поверителността на защитени компютърни данни

Отговор: Г

**39) Фишингът е форма на**

A) подправяне. (spoofing)

Б) регистриране. (logging)

В) проследяване. (Sniffing)

Г) задвижване. (Driving)

Отговор: A

**40) Пример за фишинг е**

А) създаване на фалшива гореща точка на Wi-Fi.

Б) създаване на фалшив медицински уебсайт, който иска от потребителите поверителна информация.

В) преструване на служител на компания за комунални услуги, за да се получи информация от тази компания за нейната система за сигурност.

Г) изпращане на масово електронно писмо, в което под фалшив претекст се иска финансова помощ.

Отговор: Б

**41) Злите близнаци са:**

A) Троянски коне, които изглеждат като легитимни търговски софтуерни приложения.

B) имейл съобщения, които имитират имейлите на легитимен бизнес.

C) измамни уебсайтове, които имитират уебсайта на легитимен бизнес.

D) фалшиви точки за достъп до безжична мрежа, които изглеждат легитимни за потребителите.

Отговор: D

**42) Фарминг включва:**

A) пренасочване на потребителите към измамен уебсайт, дори когато потребителят е въвел правилния адрес в уеб браузъра.

B) преструване на представител на легитимен бизнес с цел получаване на информация за система за сигурност.

C) създаване на фалшиви уебсайтове, които искат поверителна информация от потребителите.

D) използване на имейли за заплахи или тормоз.

Отговор: A

**43) Като консултант по сигурността за адвокатска кантора, кое от следните представлява най-голям източник на заплахи за сигурността на фирмата?**

A) безжична мрежа

B) служители

C) процедури за автентификация

D) липса на криптиране на данни

Отговор: B

**44) Измамване на служители да разкрият паролите си чрез преструване на легитимен член на компанията се нарича:**

A) подслушване.

B) социално инженерство.

C) фишинг.

D) фарминг.

Отговор: B

**45) Как софтуерните доставчици коригират недостатъци в своя софтуер след като е разпространен?**

A) издават корекции на грешки.

B) издават пачове.

C) преиздават софтуера.

D) издават актуализирани версии.

Отговор: B

**46) Законът HIPAA от 1997 г.:**

A) изисква финансовите институции да осигурят сигурността на клиентските данни.

B) определя най-добрите практики в сигурността и контрола на информационните системи.

C) налага отговорност на компаниите и управлението да защитават точността на финансовата информация.

D) очертава правила за медицинска сигурност и поверителност.

Отговор: D

**47) Законът Gramm-Leach-Bliley:**

A) изисква финансовите институции да осигурят сигурността на клиентските данни.

B) определя най-добрите практики в сигурността и контрола на информационните системи.

C) налага отговорност на компаниите и управлението да защитават точността на финансовата информация.

D) очертава правила за медицинска сигурност и поверителност.

Отговор: A

**48) Законът Sarbanes-Oxley:**

A) изисква финансовите институции да осигурят сигурността на клиентските данни.

B) определя най-добрите практики в сигурността и контрола на информационните системи.

C) налага отговорност на компаниите и управлението да защитават точността на финансовата информация.

D) очертава правила за медицинска сигурност и поверителност.

Отговор: C

**49) Най-често срещаният вид електронни доказателства е**:

A) гласова поща. B) електронни таблици. C) мигновени съобщения. D) имейл.

Отговор: D

**50) Електронни доказателства върху компютърни носители, които не са видими за обикновения потребител, се наричат \_\_\_\_\_\_ данни.**

A) дефрагментирани B) околни C) форензични D) фрагментирани

Отговор: B

**51) Контролите на приложенията:**

A) могат да бъдат класифицирани като входни контроли, контроли на обработката и изходни контроли.

B) управляват дизайна, сигурността и използването на компютърни програми и сигурността на файлове с данни в цялата организация.

C) се прилагат за всички компютъризирани приложения и се състоят от комбинация от хардуер, софтуер и ръчни процедури, които създават обща контролна среда.

D) включват софтуерни контроли, контроли на компютърните операции и контроли на внедряване.

Отговор: A

**52) \_\_\_\_\_\_ контроли осигуряват, че ценните бизнес файлове с данни на диск или лента не са подложени на неразрешен достъп, промяна или унищожение, докато са в употреба или в съхранение.**

A) Софтуерни

B) Административни

C) Контроли за сигурност на данните

D) Контроли за внедряване

Отговор: C

**53) Анализът на информационна система, който оценява вероятността за настъпване на инцидент със сигурността и неговата цена, е включен в:**

A) политика за сигурност.

B) Приемлива Политика за Ползване (AUP).

C) оценка на риска.

D) бизнес анализ на въздействието.

Отговор: C

**54) \_\_\_\_\_\_\_\_\_\_ се използва за идентифициране и упълномощаване на различни категории потребители на системата и за специфициране на кои части от системите на организацията всеки потребител може да има достъп.**

A) система за управление на идентичността

B) AUP

C) автентификация

D) защитна стена

Отговор: A

**55) Кое от следните не е една от основните техники за филтриране на защитни стени?**

A) филтриране на приложни проксита

B) статично филтриране на пакети

C) NAT

D) филтриране на защитен сокет

Отговор: D

**56) Стриктните системи за пароли:**

A) са едни от най-ефективните инструменти за сигурност.

B) могат да възпрепятстват производителността на служителите.

C) са скъпи за внедряване.

D) често се пренебрегват от служителите.

Отговор: B

**57) Токен за автентификация е:**

A) устройство с размер на кредитна карта, което съдържа данни за разрешения за достъп.

B) вид смарт карта.

C) устройство, което показва пароли.

D) електронен маркер, прикрепен към цифров файл за упълномощаване.

Отговор: C

**58) Кое от следните не е характеристика, използвана за идентификация в биометрични системи**?

A) изображение на ретината

B) глас

C) цвят на косата

D) лице

Отговор: C

**59) Защитната стена позволява на организацията да**:

A) предотвратява неразрешена комуникация както в мрежата, така и извън нея.

B) наблюдава мрежови горещи точки за признаци на нарушители.

C) предотвратява влизането на известен шпионски и зловреден софтуер в системата.

D) всички гореизброени.

Отговор: A

**60) При кой метод на шифроване е изпратен един ключ за шифроване до получателя, така че както изпращачът, така и получателят да споделят един и същ ключ?**

A) SSL

B) симетрично шифроване на ключове

C) публично шифроване на ключове

D) частно шифроване на ключове

Отговор: B

**61) \_\_\_\_\_\_ използват софтуер за сканиране, за да търсят известни проблеми като лоши пароли, премахването на важни файлове, атаки на сигурността в процес и грешки в системната администрация.**

A) Статични инспекции

B) Системи за откриване на прониквания

C) Технологии за филтриране на приложни проксита

D) Технологии за филтриране на пакети

Отговор: B

**62) В момента протоколите, използвани за сигурно предаване на информация в Интернет, са:**

A) TCP/IP и SSL. B) S-HTTP и CA. C) HTTP и TCP/IP. D) SSL, TLS и S-HTTP.

Отговор: D

**63) Повечето антивирусни програми са ефективни срещу:**

A) само тези вируси, които са активни в Интернет и чрез имейл.

B) всеки вирус.

C) всеки вирус, освен тези в приложенията за безжични комуникации.

D) само тези вируси, които са вече известни, когато софтуерът е написан.

Отговор: D

**64) При кой метод на криптиране на получателя се изпраща един-единствен ключ за криптиране, така че и изпращачът, и получателят да споделят един и същ ключ?**

A) SSL

B) криптиране със симетричен ключ

C) криптиране с публичен ключ

D) криптиране с частен ключ

Отговор: B

**65) Система за цифрови сертификати:**

A) използва трети страни CA за удостоверяване на самоличността на потребителя.

B) използва цифрови подписи за удостоверяване на самоличността на потребителя.

C) използва токени за удостоверяване на самоличността на потребителя.

D) се използва основно от индивиди за лична кореспонденция.

Отговор: A

**66) Прекъсването на работата (downtime) се отнася за периоди от време, в които:**

A) компютърната система работи неправилно.

B) компютърната система не е оперативна.

C) компанията или организацията не е оперативна.

D) компютърът не е онлайн.

Отговор: B

**67) За 100% наличност, онлайн транзакционната обработка изисква:**

A) висококапацитетно съхранение.

B) мрежа от сървъри на няколко нива.

C) компютърни системи с устойчивост на откази.

D) специализирани телефонни линии.

Отговор: C

**68) При контрола на мрежовия трафик за минимизиране на забавянията се използва технология, наречена \_\_\_\_\_\_, която изследва файловете с данни и сортира данни с нисък приоритет от данни с висок приоритет.**

A) компютинг с висока наличност

B) дълбока инспекция на пакети

C) филтриране на приложни проксита

D) състояние на инспекция

Отговор: B

**69) Разработването и използването на методи, които позволяват на компютърните системи да възобновят дейността си по-бързо след неуспехи, се нарича:**

A) компютинг с висока наличност.

B) компютинг, ориентиран към възстановяване.

C) компютинг с устойчивост на откази.

D) планиране на възстановяване от бедствия.

Отговор: B

**70) По-малките фирми могат да възложат на външни изпълнители някои или много функции за сигурност на:**

A) Интернет доставчици (ISPs).

B) Управление на информационните системи (MISs).

C) Доставчици на управлявани услуги за сигурност (MSSPs).

D) Удостоверяващи органи (CAs).

Отговор: C

# СВОБОДНИ ОТГОВОРИ

**71) Практиката, при която подслушвачите обикалят сгради или паркират отвън и се опитват да прихванат безжичен мрежов трафик, се нарича \_\_\_\_\_\_.**

Отговор: War driving (обикаляне за прихващане на сигнали)

**72) Злонамерени софтуерни програми, известни като \_\_\_\_\_\_, включват различни заплахи като компютърни вируси, червеи и Троянски коне.**

Отговор: Зловреден софтуер (malware)

**73) \_\_\_\_\_\_ е престъпление, при което измамник получава ключови лични данни, за да се представи за друг човек.**

Отговор: Кражба на самоличност (Identity theft)

**74) Научната колекция, изследване, удостоверяване, съхранение и анализ на данни, съхранявани на или извлечени от компютърни носители, по начин, който позволява информацията да бъде използвана като доказателство в съда, се нарича \_\_\_\_\_\_.**

Отговор: Компютърна форензика

**75) В общи линии \_\_\_\_\_\_ контроли се прилагат за всички компютризирани приложения и се състоят от комбинация от хардуер, софтуер и ръчни процедури, които създават обща контролна среда.**

Отговор: Общи (General)

**76) \_\_\_\_\_\_ преглежда общата сигурност на фирмата, както и контролите, които управляват отделните информационни системи.**

Отговор: Аудит на информационните системи (MIS audit)

**77) \_\_\_\_\_\_ се отнася до способността да се знае, че човек е този, за когото се представя.**

Отговор: Удостоверяване (Authentication)

**78) Комплексните продукти за управление на сигурността, с инструменти за защитни стени, VPN, системи за откриване на прониквания и други, се наричат \_\_\_\_\_\_ системи.**

Отговор: Системи за обединено управление на заплахи (Unified threat management)

**79) PKI е използването на публична ключова криптография, работеща с \_\_\_\_\_\_.**

Отговор: Удостоверяващ орган (Certificate Authority)

**80) Когато се открият грешки в софтуерни програми, източниците на грешките се намират и отстраняват чрез процес, наречен \_\_\_\_\_\_.**

Отговор: Дебъгване (Debugging)