نام: _____ تاریخ: _____ نمره: _____

حفاظت از داده و ذخیره‌سازی سازمانی راهنمای امنیت

پوشانی داده، توکن‌سازی، رمزگذاری در حالت سکون در برابر رمزگذاری در حال انتقال، پشتیبان‌گیری آفلاین

مرور آموزشی حفاظت از داده

خوش آمدید! این بستهٔ فعالیت شما را در بررسی استانداردها و کنترل‌های حفاظت از داده راهنمایی می‌کند. با رمزگذاری کامل دیسک، کنترل‌های دسترسی امن، پشتیبان‌گیری سخت‌افزاری، وضعیت امنیت ابری و روش‌های ماسک کردن داده آشنا می‌شوید.

ایمن‌شده
رمزگذاری داده
استاندارد AES 256 بیتی

منطبق
استانداردهای جهانی
چارچوب‌های GDPR و CCPA

اعتماد صفر
سیاست دسترسی
احراز هویت چندعاملی

ایستگاه‌های بررسی کاربرگ

- [ ] **بخش 1-4: بر امنیت سایبری و پیشگیری از تهدید مسلط شوید.**
- [ ] **بخش 5-7: جدول‌های متقاطع و جدول‌های جست‌وجوی کلمه را حل کنید.**
- [ ] **بخش 8-9: مطالعات موردی و چالش رمز را حل کنید.**
- [ ] **بخش 10: صفحه‌های پرسش‌های متداول مقدماتی و پیشرفته را مرور کنید.**
- [ ] **بخش 11: 10 واقعیت جالب دنیای واقعی را کاوش کنید.**
- [ ] **تکمیلی: چالش سریع فکر کن**

باز کردن راهنمای امنیت سایبری VPN.com

URL: https://www.vpn.com/cybersecurity/data-protection/

نقشهٔ راه یادگیری راهبرد حفاظت از داده شما

- میان تکنیک‌های پوشانی داده و توکن‌سازی تمایز قائل شوید.
- رمزگذاری در حالت ذخیره را برای درایوهای ذخیره‌سازی و رمزگذاری در حین انتقال را با TLS پیاده‌سازی کنید.
- سامانه‌های پشتیبان آفلاین و جداشده از شبکه را برای محافظت در برابر باج‌افزار طراحی کنید.

دستورالعمل‌های راهنمای حفاظت از داده

به پرسش‌های چندگزینه‌ای و درست/نادرست پاسخ دهید، جمله‌های جای‌خالی را با استفاده از بانک واژه‌ها کامل کنید، تعاریف را تطبیق دهید و جدول‌های کلمات متقاطع و جست‌وجوی کلمه را حل کنید. دانسته‌های خود را درباره حفاظت از داده‌ها به کار ببرید. و در پایان، فعالیت تکمیلی «سریع فکر کن».

حفاظت از داده و امنیت ذخیره‌سازی سازمانی (مقدمه)

حفاظت از داده، دارایی‌های داده‌ای سازمان را از طریق پوشانی، توکن‌سازی، رمزگذاری پایگاه داده در حالت سکون و پروتکل‌های امن انتقال محافظت می‌کند. طراحی پشتیبان‌های جداشده از شبکه کمک می‌کند در صورت نفوذ فعال، پایگاه‌های دادهٔ کلیدی قابل بازیابی باشند.

هر ایستگاه بررسی را با دقت بخوانید و پاسخ درست را انتخاب کنید یا بنویسید.

ایستگاه بررسی 1: چالش چندگزینه‌ای

1. هدف اصلی پوشاندن داده (data masking) چیست؟

- A. جایگزینی شناسه‌های حساس با نویسه‌های ساختگی اما واقع‌نما برای حفظ حریم خصوصی
- B. فشرده‌سازی فایل‌های بزرگ پایگاه داده برای صرفه‌جویی در فضای ذخیره‌سازی فیزیکی سرور
- C. حذف ایمیل‌های قدیمی تماس مشتریان از سامانه‌های پشتیبان بایگانی
- D. پنهان کردن IP عمومی سرور پایگاه داده از اسکن‌های اینترنتی

2. کدام سازوکار فایل‌های ذخیره‌شده روی هارد درایو سرور پایگاه داده را رمزگذاری می‌کند؟

- A. رمزگذاری کامل دیسک در حالت ذخیره
- B. پروتکل‌های دست‌دهی نشست TLS هنگام انتقال
- C. قوانین ارسال سرور نام DNS پویا
- D. احراز هویت چندعاملی با کلیدهای سخت‌افزاری

3. چه چیزی نمایندهٔ داده در حال انتقال است؟

- A. بسته‌های دادهٔ در حال حرکت در روترها و سوئیچ‌های شبکه
- B. لاگ‌های تراکنش پایگاه داده که روی یک درایو پشتیبان سرد ذخیره شده‌اند
- C. فایل‌های کاربری بایگانی‌شده که در یک گاوصندوق ابری جداشده ذخیره شده‌اند
- D. فایل‌های پیکربندی ایستای سیستم روی ذخیره‌ساز رومیزی محلی

4. چرا پشتیبان آفلاین منظم برای محافظت در برابر باج‌افزار حیاتی است؟

- A. نسخهٔ تمیز و آفلاین فراهم می‌کند تا فایل‌ها بدون پرداخت باج بازیابی شوند
- B. از اسکن پیکربندی پورت‌های باز توسط هکرها جلوگیری می‌کند
- C. سرعت پهنای باند انتقال شبکهٔ محلی را افزایش می‌دهد
- D. لاگ‌های انتخاب رضایت کوکی را در مرورگرها خودکار می‌کند

5. توکن‌سازی داده چه کاری انجام می‌دهد؟

- A. شمارهٔ کارت‌های حساس را با توکن‌های تصادفی غیرحساس جایگزین می‌کند
- B. ترافیک وب را از طریق چندین گرهٔ پیازی امن مسیریابی می‌کند
- C. پوشه‌های سیستم را برای یافتن بدافزارهای مبتنی بر امضا اسکن می‌کند
- D. زمان نشست ورود مدیران پایگاه داده را ممیزی می‌کند

ایستگاه بررسی 2: چالش درست یا نادرست

پرسش 6

6. پوشانی داده، رکوردهای پایگاه داده را در محیط‌های عملیاتی به‌طور دائمی تغییر می‌دهد.

درست نادرست

پرسش 7

7. پشتیبان‌های بیرونی باید از شبکهٔ اصلی سازمان جدا باشند تا از گسترش باج‌افزار جلوگیری شود.

درست نادرست

پرسش 8

8. گواهی‌های SSL/TLS با رمزگذاری داده‌های ذخیره‌شده روی رسانهٔ فیزیکی از پایگاه‌های داده محافظت می‌کنند.

درست نادرست

پرسش 9

9. دسترسی شبکهٔ اعتماد صفر (ZTNA) پیش از اعطای دسترسی به پایگاه داده، هویت هر کاربر را راستی‌آزمایی می‌کند.

درست نادرست

پرسش 10

10. توکن‌سازی مبتنی بر خزانه (vault-based) مقادیر اصلی کارت را در یک خزانهٔ توکن مرکزی و امن ذخیره می‌کند.

درست نادرست

ایستگاه بررسی 3: درج اصطلاح کلیدی

هر جملهٔ زیر را بخوانید و جای خالی را با واژهٔ درست از بانک واژگان پر کنید.

1. جایگزین کردن نام‌های شخصی با جانشین‌های واقع‌نما، _____ داده نامیده می‌شود.
2. رمزگذاری بلوک‌های ذخیره‌سازی فیزیکی از دارایی‌های پایگاه داده در حال _____ محافظت می‌کند.
3. پروتکل‌های TLS بسته‌های داده فعال را که در حال _____ هستند رمزگذاری می‌کنند.
4. مجوزهای مبتنی بر نقش تعیین می‌کنند کدام کاربران می‌توانند به پایگاه داده _____ پیدا کنند.
5. بازیابی فایل‌های سالم شرکت پس از نقض امنیتی به یک _____ آفلاین امن نیاز دارد.
6. ممیزی پیکربندی‌های ابری _____ امنیتی یک سازمان را ارزیابی می‌کند.

بانک واژگان

انتقال | انطباق | پوشانی | دسترسی | رخنه | سکون | نسخهٔ پشتیبان | وضعیت

پاسخ‌های خود را اینجا بنویسید:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____

ایستگاه بررسی 4: تطبیق مفاهیم امنیت

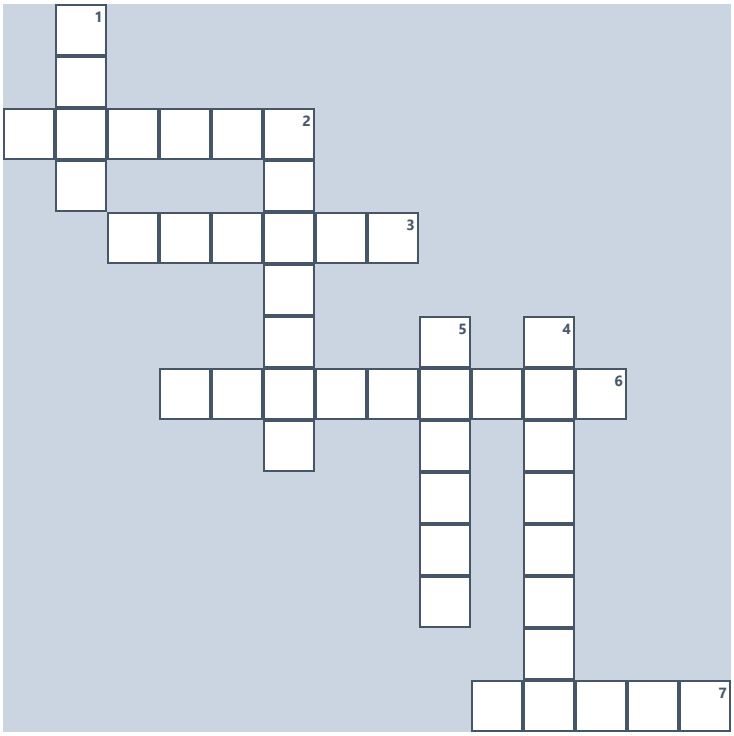
تطبیق تعاریف

هر اصطلاح واژگان در سمت راست را با نوشتن حرف متناظر (A-H) در کادر ورودی قابل‌پرکردن به تعریف درست آن در سمت چپ وصل کنید.

1. رمزگذاری	A	ایجاد نسخه‌های امن بیرونی از داده‌ها برای بازیابی در صورت خرابی سیستم.
2. پشتیبان	B	تبدیل متن ساده به متن رمزشدهٔ ناخوانا تا داده‌های رهگیری‌شده خصوصی بمانند.
3. کمینه‌سازی	C	وضعیت امنیتی و آمادگی دفاعی جمعی ابر یک سازمان.
4. دسترسی	D	رعایت استانداردهای مقرراتی مانند GDPR یا CCPA برای مدیریت اطلاعات خصوصی کاربران.
5. وضعیت امنیتی	E	رخداد امنیتی که در آن داده‌های محافظت‌شده بدون مجوز مورد دسترسی قرار می‌گیرند یا افشا می‌شوند.
6. نقض امنیتی	F	محدودکردن مجوزهای خواندن و نوشتن پایگاه داده به نقش‌های کاربری احراز هویت‌شده.
7. انطباق	G	جایگزینی نویسه‌های حساس در فیلدهای پایگاه داده برای حفاظت از هویت‌های شخصی.
8. پنهان‌سازی	H	محدود کردن گردآوری داده‌های شخصی به حداقل مطلق لازم برای عملیات.

ایستگاه بررسی 5: جدول‌کلمات

جدول کلمات متقاطع را با تایپ حروف در خانه‌های سفید فعال حل کنید. شماره‌ها با سرنخ‌های زیر مطابقت دارند.



افقی

2. جایگزین کردن نویسه‌های حساس در فیلدهای پایگاه داده برای محافظت از هویت افراد (6)

3. محدود کردن مجوزهای خواندن و نوشتن پایگاه داده به نقش‌های کاربری احرازشده (6)

6. محدود کردن گردآوری داده‌های شخصی به حداقل مطلق لازم برای عملیات (9)

7. حالت امنیتی جمعی و آمادگی دفاعی ابر یک سازمان (5)

عمودی

1. رویداد امنیتی که در آن داده‌های محافظت‌شده بدون مجوز در دسترس قرار می‌گیرند یا افشا می‌شوند (4)

2. ساخت نسخه‌های امن بیرون از محل داده برای بازیابی در صورت خرابی سیستم (7)

4. تبدیل متن ساده به رمزنوشت ناخوانا تا داده‌های شنودشده خصوصی بمانند (8)

5. رعایت استانداردهای مقرراتی مانند GDPR یا CCPA برای مدیریت اطلاعات خصوصی کاربران (6)

ایستگاه بررسی 5 – فعالیت جایگزین: سرنخ‌های دسترس‌پذیر جدول‌کلمات

کاربران صفحه‌خوان و صفحه‌کلید می‌توانند پاسخ‌های جدول کلمات متقاطع را مستقیماً در فیلدهای متنی زیر تایپ کنند.

افقی

2 افقی: جایگزین کردن نویسه‌های حساس در فیلدهای پایگاه داده برای محافظت از هویت افراد (6 حرف):

3 افقی: محدود کردن مجوزهای خواندن و نوشتن پایگاه داده به نقش‌های کاربری احرازشده (6 حرف):

6 افقی: محدود کردن گردآوری داده‌های شخصی به حداقل مطلق لازم برای عملیات (9 حرف):

7 افقی: حالت امنیتی جمعی و آمادگی دفاعی ابر یک سازمان (5 حرف):

عمودی

1 عمودی: رویداد امنیتی که در آن داده‌های محافظت‌شده بدون مجوز در دسترس قرار می‌گیرند یا افشا می‌شوند (4 حرف):

2 عمودی: ساخت نسخه‌های امن بیرون از محل داده برای بازیابی در صورت خرابی سیستم (7 حرف):

4 عمودی: تبدیل متن ساده به رمزنوشت ناخوانا تا داده‌های شنودشده خصوصی بمانند (8 حرف):

5 عمودی: رعایت استانداردهای مقرراتی مانند GDPR یا CCPA برای مدیریت اطلاعات خصوصی کاربران (6 حرف):

ایستگاه بررسی 6: جدول کلمات پنهان

8 اصطلاح کلیدی واژگان را که در جدول زیر پنهان شده‌اند پیدا کنید. کلمات می‌توانند افقی، عمودی یا مورب باشند.

ف	ک	ت	ض	ع	ن	ظ	ش	غ	ص	ح	ذ	ی	غ	ت
و	ز	ژ	و	ط	پ	د	ب	ا	پ	ر	ژ	ن	ج	ق
ژ	ص	ص	ذ	ث	س	ر	ش	ع	ث	ز	ک	ا	ن	ژ
غ	ع	ش	ش	ت	خ	ا	ن	ط	ب	ا	ق	ش	ظ	ع
م	پ	ف	ر	د	ض	ظ	ف	پ	ک	خ	ک	و	ک	ف
ز	ح	س	م	ی	ت	ت	ر	گ	م	ه	ق	پ	ث	ن
گ	ی	پ	ظ	ی	ن	م	ع	ث	ی	ص	ث	ی	خ	ا
چ	ث	ض	ع	ث	ز	ا	ژ	ث	ن	ض	ی	ا	ب	ب
ق	ی	ض	ف	گ	ذ	ج	ش	ع	ه	غ	ث	ذ	خ	ی
ظ	و	ص	ذ	ط	ع	ا	ا	ر	س	چ	ل	ع	چ	ت
پ	ه	ا	ص	ت	ف	ک	غ	خ	ا	ز	ع	و	ک	ش
ژ	ر	ه	ه	ی	غ	ا	ر	ن	ز	م	ن	ف	ح	پ
ی	ع	ظ	خ	ط	ق	س	س	ه	ی	ز	غ	ش	ذ	ح
ی	س	خ	ب	ه	ف	ه	پ	گ	ح	ل	ض	ا	ی	خ
گ	م	ط	و	ح	ه	ی	س	پ	ن	ص	ظ	ض	ز	خ

فهرست واژگان

رمزگذاری　پشتیبان　کمینه‌سازی　دسترسی　وضعیت　رخنه　انطباق　پوشانی

ایستگاه بررسی 6 – فعالیت جایگزین: تطبیق دسترس‌پذیر واژگان

هر یک از 8 اصطلاح واژگان موجود در جدول کلمات پنهان را با نوشتن حرف (A-H) در جای خالی به تعریف درست آن وصل کنید.

اصطلاحات واژگان	تعاریف و فیلدهای تطبیق
A. رمزگذاری	1. رویداد امنیتی که در آن داده‌های محافظت‌شده بدون مجوز در دسترس قرار می‌گیرند یا افشا می‌شوند.
B. پشتیبان	2. جایگزین کردن نویسه‌های حساس در فیلدهای پایگاه داده برای محافظت از هویت افراد.
C. کمینه‌سازی	3. محدود کردن مجوزهای خواندن و نوشتن پایگاه داده به نقش‌های کاربری احرازشده.
D. دسترسی	4. حالت امنیتی جمعی و آمادگی دفاعی ابر یک سازمان.
E. وضعیت	5. رعایت استانداردهای مقرراتی مانند GDPR یا CCPA برای مدیریت اطلاعات خصوصی کاربران.
F. رخنه	6. محدود کردن گردآوری داده‌های شخصی به حداقل مطلق لازم برای عملیات.
G. انطباق	7. تبدیل متن ساده به رمزنوشت ناخوانا تا داده‌های شنودشده خصوصی بمانند.
H. پوشانی	8. ساخت نسخه‌های امن بیرون از محل داده برای بازیابی در صورت خرابی سیستم.

ایستگاه بررسی 7: چالش کلمات درهم‌ریخته

حروف زیر را مرتب کنید تا مفاهیم و اصطلاحات کلیدی امنیت سایبری آشکار شوند. پاسخ‌هایتان را در کادرهای ورودی ارائه‌شده بنویسید.

1. ر گ ذ ر ا م ی ز _____
2. ی ک ز ن م س ا ه ی _____
3. ع و ت ی ض _____
4. ق ب ط ا ا ن _____
5. ب ن ی ت پ ا ش _____
6. س ر د ت ی س _____
7. ن ر ه خ _____
8. ش ی پ ن ا و _____

فعالیت تکمیلی: سریع فکر کن

برای هر دسته 3 پاسخ بنویسید. هر کس زودتر فهرست را کامل کند برنده است.

1	چیزهایی که پشتیبان می‌گیرید		
2	واژه‌های مرتبط با امنیت سایبری		
3	افرادی که مجاز به دیدن داده‌های حساس‌اند		
4	روش‌های حذف امن داده		
5	جاهایی که داده ذخیره می‌شود		
6	چیزهایی که باید رمزگذاری شوند		
7	داده‌هایی که یک بیمارستان باید محافظت کند		
8	انواع پشتیبان		
9	اطلاعاتی که هرگز نباید به اشتراک بگذارید		
10	نشانه‌های هشدار در یک ایمیل		
11	عادت‌های ایمن که می‌توانید از امروز شروع کنید		
12	افرادی که می‌توانید برای کمک فناوری اطلاعات از آن‌ها بپرسید		
13	دستگاه‌هایی که می‌توانند هک شوند		
14	روش‌های محافظت از داده		
15	چیزهایی که می‌توانند داده را نابود کنند		

ایستگاه بررسی 8: مطالعات موردی امنیت سایبری

مفاهیمی را که آموخته‌اید برای حل سناریوهای واقعی زیر به کار ببرید.

مطالعهٔ موردی 1: ارتقای رمزگذاری پایگاه داده سازمانی در حالت سکون



سناریو: یک خرده‌فروش آنلاین پایگاه‌های داده تراکنش را بدون رمزگذاری کامل دیسک روی ذخیره‌سازی ابری نگه می‌دارد. یک ممیزی انطباق اخیر این را یک ریسک جدی امنیت داده در CCPA علامت‌گذاری کرد. یک معماری بازیابی طراحی کنید.

پرسش برای بحث: ریسک‌های انطباق با CCPA را تحلیل کنید و یک راهبرد رمزگذاری داده در حالت ذخیره پیشنهاد دهید.

مطالعهٔ موردی 2: مهار باج‌افزار و بازیابی داده‌ها



سناریو: یک حملهٔ فعال باج‌افزار در حال رمزگذاری درایوهای شبکه در یک شبکهٔ محلی شرکتی است. مدیر آلودگی را زود شناسایی کرده است. مراحل مهار و بازیابی را برنامه‌ریزی کنید.

پرسش برای بحث: اقدامات فوری مهار را شرح دهید و یک فرایند بازیابی امن را برنامه‌ریزی کنید.

ایستگاه بررسی 9: رمزگشایی

متخصص امنیت سایبری از دارایی‌های شبکه در برابر عوامل تهدید آنلاین محافظت می‌کند. از کلید حرف-به-عدد زیر استفاده کنید و با نوشتن حرف‌های متناظر در جاهای خالی، پیام را رمزگشایی کنید.

کلید رمزگذاری حرف به عدد

ا=1 ب=2 پ=3 ت=4 ث=5 ج=6 چ=7 ح=8 خ=9 د=10 ذ=11

ر=12 ز=13 ژ=14 س=15 ش=16 ص=17 ض=18 ط=19 ظ=20 ع=21 غ=22

ف=23 ق=24 ک=25 گ=26 ل=27 م=28 ن=29 و=30 ه=31 ی=32

31	10	1	10		13	1		29	28	1		27	12	4	29	25		1	2

4	20	23	1	8	28

پیام رمزگشایی‌شده:

نکته: هر عدد نشان‌دهندهٔ یک حرف فارسی از کلید بالا است.

ایستگاه بررسی 10: پرسش‌های متداول امنیت سایبری – مقدماتی (بخش A)

پرسش‌ها و پاسخ‌های رایج دربارهٔ کاهش تهدیدهای آنلاین را مرور کنید.

Q1: حفاظت از داده چیست؟

فرایند محافظت از داده‌های شخصی و تجاری در برابر دسترسی غیرمجاز، از دست رفتن یا خرابی از طریق کنترل‌های فنی است.

Q2: چرا رمزگذاری کامل دیسک مهم است؟

بلوک‌های داده ذخیره‌شده روی درایوهای فیزیکی را ایمن می‌کند و در صورت دزدیده شدن فیزیکی هارددیسک، مانع از خواندن داده توسط هر کسی می‌شود.

Q3: تفاوت رمزگذاری در حالت ذخیره و در حال انتقال چیست؟

رمزگذاری در حالت سکون فایل‌های ذخیره‌شده روی درایوها را ایمن می‌کند، در حالی که رمزگذاری در حال انتقال بسته‌های فعال شبکه را که روی روترها جابه‌جا می‌شوند ایمن می‌کند.

Q4: پوشانی داده چیست؟

جزئیات حساس (مانند شماره‌های کارت اعتباری) را با داده‌های ساختگی اما واقع‌نما جایگزین می‌کند تا آزمون بدون افشای سوابق واقعی انجام شود.

Q5: چرا پشتیبان آفلاین مهم است؟

یک نسخهٔ سالم از فایل‌های شما را جدا از شبکه نگه می‌دارد که به محافظت از پشتیبان‌های شما در برابر رمزگذاری توسط باج‌افزار کمک می‌کند.

ایستگاه بررسی 10: پرسش‌های متداول امنیت سایبری – مقدماتی (بخش B)

پرسش‌ها و پاسخ‌های رایج دربارهٔ کاهش تهدیدهای آنلاین را مرور کنید.

Q6: صندوق توکن‌سازی داده چیست؟

پایگاه دادهٔ امن و ایزوله که توکن‌های تصادفی را به مقادیر حساس اصلی آن‌ها (مانند شمارهٔ اصلی کارت اعتباری) نگاشت می‌کند.

Q7: دسترسی اعتماد صفر به پایگاه داده به چه معناست؟

یعنی هویت و وضعیت دستگاه هر کاربر در هر ورود راستی‌آزمایی می‌شود، به‌جای اینکه به هر کسی داخل شبکه اعتماد شود.

Q8: TLS چگونه از داده‌ها در حال انتقال محافظت می‌کند؟

TLS بار نشست TCP را رمزگذاری می‌کند و مانع از آن می‌شود که عوامل مخرب در شبکه‌های عمومی بسته‌های در حال عبور را شنود یا تغییر دهند.

Q9: ممیزی دسترسی به پایگاه داده چیست؟

ثبت پیوستهٔ پرس‌وجوها و ورودهای پایگاه داده برای شناسایی الگوهای دسترسی غیرمجاز یا ناهنجاری‌های امنیتی.

Q10: ممیزی وضعیت امنیت ابری چیست؟

فرایند تحلیل پیکربندی‌های ابری برای شناسایی درگاه‌های باز، قواعد دسترسی نادرست پیکربندی‌شده و شکاف‌های انطباق امنیتی.

ایستگاه بررسی 10: پرسش‌های متداول امنیت – پیشرفته (بخش C)

جنبه‌های فنی پیشرفتهٔ چارچوب‌های امنیتی، تحلیل بدافزار و انطباق داده را بررسی کنید.

Q1: رمزگذاری پاکتی (envelope encryption) چگونه کار می‌کند؟

داده‌ها را با کلید داده رمزگذاری می‌کند، سپس آن کلید داده را با کلید اصلی رمزگذاری می‌کند و ذخیره‌سازی و چرخش کلید را ساده می‌کند.

Q2: رمزگذاری همریخت (homomorphic) چیست؟

روش رمزگذاری پیشرفته‌ای که اجازه می‌دهد عملیات مستقیماً روی داده‌های رمزگذاری‌شده و بدون رمزگشایی اولیه انجام شود.

Q3: چرا از رمزگذاری سطح ستون پایگاه داده استفاده می‌شود؟

ستون‌های حساس مشخص (مانند SSN) را به‌طور جداگانه رمزگذاری می‌کند و حتی اگر مدیران دسترسی خواندن عمومی جدول را به دست آورند، از آنها محافظت می‌کند.

Q4: پیشگیری از نشت داده (DLP) چیست؟

نرم‌افزاری که نقاط خروج شبکه را پایش می‌کند تا انتقال‌های خروجی غیرمجاز فایل‌های حساس را شناسایی و مسدود کند.

Q5: پشتیبان‌های یک‌بارنویسی چندبارخوانی (WORM) چگونه در برابر باج‌افزار محافظت می‌کنند؟

پشتیبان‌های WORM مانع حذف یا تغییر فایل‌ها در یک مدت مشخص می‌شوند و از رمزگذاری پشتیبان‌های موجود توسط باج‌افزار جلوگیری می‌کنند.

ایستگاه بررسی 10: پرسش‌های متداول امنیت – پیشرفته (بخش D)

جنبه‌های فنی پیشرفتهٔ چارچوب‌های امنیتی، تحلیل بدافزار و انطباق داده را بررسی کنید.

Q6: خطر استفادهٔ مجدد از کلید چیست؟

استفادهٔ مجدد از یک کلید رمزنگاری در پایگاه‌های داده مختلف یعنی نفوذ به یک کلید همهٔ پایگاه‌های داده را در معرض خطر قرار می‌دهد.

Q7: توکن‌سازی پایگاه داده چگونه انطباق با CCPA را بهبود می‌دهد؟

توکن‌ها رکوردها را در سامانه‌های غیرتولیدی شبه‌ناشناس می‌کنند و در معرض قرارگیری ناشی از نشت را محدود می‌کنند، اما داده‌های توکنیزه‌شده همچنان می‌توانند اطلاعات شخصی باشند.

Q8: چرا طبقه‌بندی داده حیاتی است؟

فایل‌ها را بر اساس سطح حساسیت دسته‌بندی می‌کند و به سازمان‌ها کمک می‌کند قوی‌ترین رمزگذاری و کنترل‌های دسترسی را برای داده‌های پرخطر اعمال کنند.

Q9: نقش چرخش کلید چیست؟

به‌روزرسانی منظم کلیدهای رمزگذاری میزان داده‌های تاریخی در معرض خطر را در صورت شکسته‌شدن احتمالی یک کلید محدود می‌کند.

Q10: محفظه‌های امن چگونه از پرس‌وجوهای پایگاه داده در حافظه محافظت می‌کنند؟

enclaveهای امن، عملیات پرس‌وجو را در بلوک‌های حافظهٔ محافظت‌شده با CPU ایزوله می‌کنند و از دیدن متن آشکار در RAM توسط مدیران میزبان جلوگیری می‌کنند.

بخش 11: 10 واقعیت و بینش دنیای واقعی دربارهٔ امنیت سایبری

واقعیت‌های دنیای واقعی دربارهٔ نقض‌های امنیتی، سازوکارهای دفاعی و استانداردهای انطباق را مرور کنید.

1. بینش امنیت

مقررات GDPR در ماه مه 2018 لازم‌الاجرا شد و شیوهٔ مدیریت رضایت کوکی و ثبت داده‌های شخصی را در وب‌سایت‌های جهانی تغییر داد.

2. بینش امنیت

جریمهٔ نقض GDPR می‌تواند به 20 میلیون یورو یا 4% گردش مالی جهانی برسد که نشان‌دهندهٔ مواجهه با خطر حقوقی قابل‌توجه است. [4]

3. بینش امنیت

CCPA در ژانویهٔ 2020 لازم‌الاجرا شد و حقوق پیشگامانهٔ مصرف‌کنندگان در حوزهٔ حریم خصوصی دیجیتال را در ایالات متحده ایجاد کرد.

4. بینش امنیت

کمینه‌سازی داده، حجم ذخیره‌سازی پایگاه داده را کاهش می‌دهد و هزینه‌های عملیاتی سرور را پایین می‌آورد و در عین حال، مقیاس تأثیر نقض را کم می‌کند.

5. بینش امنیت

خرد کردن رمزنگاری چالش حذف پشتیبان را با پاک کردن کلیدها حل می‌کند، به‌جای ویرایش فایل‌های نوار پشتیبان تاریخی.

6. بینش امنیت

بیشتر کشورهای جهان اکنون قوانین حفاظت از داده‌های شخصی را برای محافظت از حقوق حریم خصوصی مصرف‌کنندگان تصویب کرده‌اند.

7. بینش امنیت

فرم‌های رضایت با گزینهٔ از پیش تیک‌خورده بر اساس تعاریف مقرراتی حریم خصوصی داده در اروپا صراحتاً ممنوع‌اند.

8. بینش امنیت

GDPR الزام می‌کند نقض داده‌های شخصی، در صورت امکان، ظرف 72 ساعت پس از آگاهی به مرجع نظارتی گزارش شود. [3]

9. بینش امنیت

هش کردن گذرواژه‌ها با الگوریتم‌های کند مانند bcrypt یا Argon2 شکستن آفلاین هش‌های دزدیده‌شده را بسیار دشوارتر می‌کند. [6]

10. بینش امنیت

داده‌های در حالت سکون همان فایل‌های ذخیره‌شدهٔ پایگاه داده هستند، در حالی که داده‌های در حال انتقال، بسته‌هایی را شامل می‌شوند که فعالانه در روترهای شبکه جابه‌جا می‌شوند.

منابع و مراجع فنی

راهنمای مطالعه و پازل‌های تعاملی از استانداردهای جهانی NIST، OWASP و انطباق با حریم خصوصی داده گردآوری شده‌اند.

منابع علمی و صنعتی

[1] NIST. (2025). SP 800-88 Rev. 2, Guidelines for Media Sanitization.
https://csrc.nist.gov/pubs/sp/800/88/r2/final

[2] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[3] Intersoft Consulting. (n.d.). Art. 33 GDPR – Notification of a personal data breach to the supervisory authority.
https://gdpr-info.eu/art-33-gdpr/

[4] Intersoft Consulting. (n.d.). Art. 83 GDPR – General conditions for imposing administrative fines.
https://gdpr-info.eu/art-83-gdpr/

[5] California Privacy Protection Agency. (n.d.). Frequently Asked Questions (FAQs).
https://cppa.ca.gov/faq.html

[6] OWASP. (n.d.). Password Storage Cheat Sheet.
https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

کلید پاسخ: ایستگاه بررسی 1 – چندگزینه‌ای

1 پرسش 1 — پاسخ درست: A

نکتهٔ آموزشی

هدف اصلی پوشاندن داده (data masking) چیست؟ → جایگزینی شناسه‌های حساس با نویسه‌های ساختگی اما واقع‌نما برای حفظ حریم خصوصی

2 پرسش 2 — پاسخ درست: A

نکتهٔ آموزشی

کدام سازوکار فایل‌های ذخیره‌شده روی هارد درایو سرور پایگاه داده را رمزگذاری می‌کند؟ → رمزگذاری کامل دیسک در حالت ذخیره

3 پرسش 3 — پاسخ درست: A

نکتهٔ آموزشی

چه چیزی نمایندهٔ داده در حال انتقال است؟ → بسته‌های دادهٔ در حال حرکت در روترها و سوئیچ‌های شبکه

4 پرسش 4 — پاسخ درست: A

نکتهٔ آموزشی

چرا پشتیبان آفلاین منظم برای محافظت در برابر باج‌افزار حیاتی است؟ → نسخهٔ تمیز و آفلاین فراهم می‌کند تا فایل‌ها بدون پرداخت باج بازیابی شوند

5 پرسش 5 — پاسخ درست: A

نکتهٔ آموزشی

توکن‌سازی داده چه کاری انجام می‌دهد؟ → شمارهٔ کارت‌های حساس را با توکن‌های تصادفی غیرحساس جایگزین می‌کند

کلید پاسخ: ایستگاه بررسی 2 – درست یا نادرست

6 **پرسش 6**

پاسخ درست: نادرست

نکتهٔ آموزشی

پوشانی (masking) نسخه‌های آزمایشی را تغییر می‌دهد یا مقادیر را در زمان پرس‌وجو پنهان می‌کند؛ رکوردهای تولیدی بدون تغییر می‌مانند.

7 **پرسش 7**

پاسخ درست: درست

نکتهٔ آموزشی

پشتیبان‌های بیرونی باید از شبکهٔ اصلی سازمان جدا باشند تا از گسترش باج‌افزار جلوگیری شود.

8 **پرسش 8**

پاسخ درست: نادرست

نکتهٔ آموزشی

گواهی‌های TLS از داده در حال انتقال محافظت می‌کنند؛ داده در حالت ذخیره به رمزگذاری دیسک، فایل یا پایگاه داده نیاز دارد.

9 **پرسش 9**

پاسخ درست: درست

نکتهٔ آموزشی

دسترسی شبکهٔ اعتماد صفر (ZTNA) پیش از اعطای دسترسی به پایگاه داده، هویت هر کاربر را راستی‌آزمایی می‌کند.

10 **پرسش 10**

پاسخ درست: درست

نکتهٔ آموزشی

توکن‌سازی مبتنی بر خزانه مقادیر اصلی را در یک خزانهٔ توکن امن نگه می‌دارد که هر توکن را به داده‌اش نگاشت می‌کند.

کلیدهای واژگان و معیار نمره‌دهی

بارم‌بندی معلم: برای هر تطبیق درست (در مجموع 8 امتیاز) و اصطلاح بافتی (در مجموع 6 امتیاز) 1 امتیاز بدهید.

ایستگاه بررسی 4: کلید پاسخ – تطبیق مفاهیم

B 1. رمزگذاری	A 2. پشتیبان	H 3. کمینه‌سازی	F 4. دسترسی
C 5. وضعیت امنیتی	E 6. نقض امنیتی	D 7. انطباق	G 8. پنهان‌سازی

ایستگاه بررسی 3: کلید پاسخ – اصطلاحات کلیدی

1 پوشانی	2 سکون	3 انتقال	4 دسترسی
5 نسخهٔ پشتیبان	6 وضعیت		

ایستگاه بررسی 6 – فعالیت جایگزین: کلید پاسخ – تطبیق واژگان

1 F – رخنه	2 H – پوشانی	3 D – دسترسی	4 E – وضعیت
5 G – انطباق	6 C – کمینه‌سازی	7 A – رمزگذاری	8 B – پشتیبان

یادداشت‌های بحث برای مدرسان

اصطلاحات کلیدی:
بررسی کنید که دانش‌آموزان بتوانند رمزگذاری، پشتیبان و کمینه‌سازی را با کلمات خودشان توضیح دهند و برای هر کدام مثالی بزنند.

مطالعات موردی:
از دانش‌آموزان بخواهید پیشنهادهای خود را بر پایهٔ واقعیت‌های کاربرگ ارائه کنند، نه نظر شخصی.

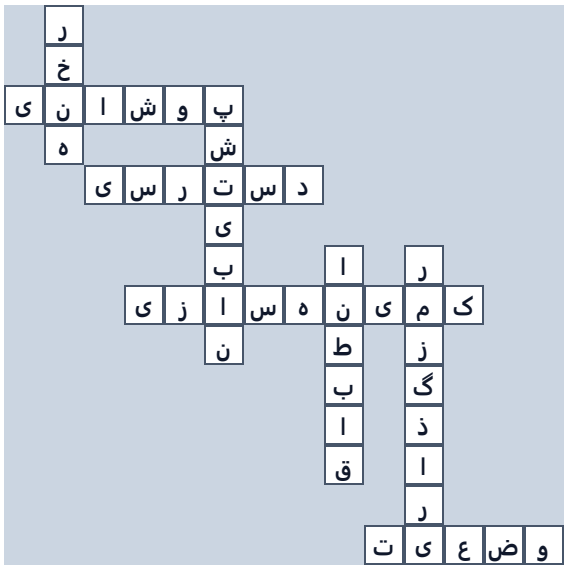
ارزیابی منابع:
از دانش‌آموزان بخواهید دست‌کم یک ادعا را در منابع کاربرگ بررسی کنند و دربارهٔ اینکه چرا ارقام، قیمت‌ها و قوانین ممکن است با گذشت زمان تغییر کنند گفت‌وگو کنید.

کلیدهای معما و یادداشت‌های معلم

پاسخ جدول کلمات

ف	ک	ت	ض	ع	ن	ظ	ش	غ	ص	ح	ذ	ی	غ	ت
و	ز	ژ	و	ط	پ	د	ب	ا	پ	ر	ژ	ن	چ	ق
ژ	ص	ص	ذ	ث	س	ر	ش	ع	ث	ز	ک	ا	ن	ژ
غ	ع	ش	ش	ت	خ	ا	ن	ط	ب	ا	ق	ش	ظ	ع
م	پ	ف	ر	د	ض	ظ	ف	پ	ک	خ	ک	و	ک	ف
ز	ح	س	م	ی	ت	ت	ر	گ	م	ه	ق	پ	ث	ن
گ	ی	پ	ظ	ی	م	ع	ث	ی	ن	ص	ث	ی	خ	ا
چ	ث	ض	ع	ث	ز	ا	ژ	ث	ن	ض	ی	ا	ب	ب
ق	ی	ض	ف	گ	ذ	چ	ش	ع	ه	غ	ث	ذ	خ	ی
ظ	و	ص	ذ	ط	ع	ا	ا	ر	س	چ	ل	ع	چ	ت
پ	ه	ا	ص	ت	ف	ک	غ	خ	ا	ز	ع	و	ک	ش
ژ	ر	ه	ه	ی	غ	ا	ر	ن	ز	م	ن	ف	ح	پ
ی	ع	خ	ط	ق	س	س	ه	ی	ز	غ	ش	ع	ذ	ح
ی	س	خ	ب	ه	ف	ه	پ	گ	ح	ل	ض	ا	ی	خ
گ	م	ط	و	ح	ه	ی	س	پ	ن	ص	ظ	ض	ز	خ

پاسخ جدول‌کلمات



راهنمای معلم برای پاسخ‌های جدول کلمات متقاطع

افقی

2 افقی: پوشانی جایگزین کردن نویسه‌های حساس در فیلدهای پایگاه داده برای محافظت از هویت افراد (6 حرف)

3 افقی: دسترسی محدود کردن مجوزهای خواندن و نوشتن پایگاه داده به نقش‌های کاربری احرازشده (6 حرف)

6 افقی: کمینه‌سازی محدود کردن گردآوری داده‌های شخصی به حداقل مطلق لازم برای عملیات (9 حرف)

7 افقی: وضعیت حالت امنیتی جمعی و آمادگی دفاعی ابر یک سازمان (5 حرف)

عمودی

1 عمودی: رخنه رویداد امنیتی که در آن داده‌های محافظت‌شده بدون مجوز در دسترس قرار می‌گیرند یا افشا می‌شوند (4 حرف)

2 عمودی: پشتیبان ساخت نسخه‌های امن بیرون از محل داده برای بازیابی در صورت خرابی سیستم (7 حرف)

4 عمودی: رمزگذاری تبدیل متن ساده به رمزنوشت ناخوانا تا داده‌های شنودشده خصوصی بمانند (8 حرف)

5 عمودی: انطباق رعایت استانداردهای مقرراتی مانند GDPR یا CCPA برای مدیریت اطلاعات خصوصی کاربران (6 حرف)

کلید پاسخ کلمات درهم‌ریخته و رمزگشایی

کلید نمره‌دهی برای فعالیت بازچینی واژگان و چالش رمز مخفی.

کلید مرتب‌سازی کلمات

1. رگذرامیز — رمزگذاری
2. یکزنمساهی — کمینهسازی
3. عوتیض — وضعیت
4. قبطاان — انطباق
5. بنیتپاش — پشتیبان
6. سردتیس — دسترسی
7. نرهخ — رخنه
8. شیپناو — پوشانی

کلید چالش رمز مخفی

"با کنترل امن از داده محافظت"

کلید پاسخ مطالعات موردی

A مطالعهٔ موردی 1: ارتقای رمزگذاری پایگاه داده سازمانی در حالت سکون

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: یک خرده‌فروش آنلاین پایگاه‌های دادهٔ تراکنش را بدون رمزگذاری کامل دیسک در فضای ذخیره‌سازی ابری نگه می‌دارد. یک ممیزی اخیر انطباق، این وضعیت را خطر جدی امنیت داده بر اساس CCPA علامت زده است. یک معماری بازیابی طراحی کنید.
- راهبرد و راه‌حل پیشنهادی: رمزگذاری کامل دیسک با AES-256 را در حالت ذخیره روی همهٔ سامانه‌های فایل اجرا کنید. از یک سرویس مدیریت کلید (KMS) متمرکز با چرخش خودکار استفاده کنید و سیاست‌های سخت‌گیرانهٔ IAM را برای کنترل دسترسی رمزگشایی اعمال کنید.

B مطالعهٔ موردی 2: مهار باج‌افزار و بازیابی داده‌ها

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: یک حملهٔ فعال باج‌افزار در حال رمزگذاری درایوهای شبکه در یک شبکهٔ محلی سازمانی است. مدیر آلودگی را زود شناسایی کرده است. مراحل مهار و بازیابی را برنامه‌ریزی کنید.
- راهبرد و راه‌حل پیشنهادی: بخش نفوذشده را فوراً ایزوله کنید. نقاط انتهایی آسیب‌دیده را فرمت کنید و از جدیدترین پشتیبان آفلاین یک‌بار-نوشتن-چندبار-خواندن (WORM) بازیابی کنید. پیش از اتصال دوبارهٔ سامانه‌ها، یکپارچگی پشتیبان را بررسی کنید.