Nome: _____ Data: _____ Pontuação: _____

Ataques de ransomware e empresas Recuperação

Execução da carga útil, encriptação criptográfica de ficheiros, cópias de segurança offline, procedimentos de contenção e recuperação de desastres.

VISÃO GERAL DE APRENDIZAGEM SOBRE ATAQUES DE RANSOMWARE

PROTEGIDO
ENCRIPTAÇÃO DE DADOS
Norma AES de 256 bits

CONFORME
NORMAS GLOBAIS
Referenciais RGPD (GDPR) e CCPA

ZERO-TRUST
POLÍTICA DE ACESSO
Autenticação multifator

Bem-vindo! Este conjunto de atividades guia-te pelos ataques de ransomware e pela recuperação empresarial. Vais explorar a execução de cargas úteis, a encriptação de ficheiros, cópias de segurança offline, a contenção de ameaças, pagamentos em criptomoedas e planos de recuperação de desastres.

PONTOS DE CONTROLO DA FICHA DE TRABALHO

- [ ] **Partes 1-4: Domina a cibersegurança e a prevenção de ameaças.**
- [ ] **Partes 5-7: Resolve puzzles de palavras cruzadas e sopas de letras.**
- [ ] **Partes 8-9: Resolve estudos de caso e o desafio de cifra.**
- [ ] **Parte 10: Revê as páginas de perguntas frequentes básicas e avançadas.**
- [ ] **Parte 11: Explora 10 factos interessantes do mundo real.**
- [ ] **Bónus: desafio Pensa rápido.**

Abrir o Guia de Cibersegurança da VPN.com

URL: https://www.vpn.com/pt/ciberseguranca/ataque-ransomware/

O teu roteiro de aprendizagem sobre recuperação de ransomware

- Distingue as cargas de Trojan, ransomware e spyware.
- Analisa ficheiros maliciosos dentro de ambientes de sandbox seguros.
- Elaborar procedimentos de isolamento e contenção rápidos da rede.

INSTRUÇÕES DO GUIA SOBRE ATAQUES DE RANSOMWARE

Responde às perguntas de escolha múltipla e de verdadeiro/falso, completa as frases de preencher espaços com o banco de palavras, associa as definições e resolve as palavras cruzadas e a sopa de letras. Aplica os teus conhecimentos à recuperação após ransomware. Termina com a atividade bónus Pensa rápido.

ATAQUES DE RANSOMWARE E RECUPERAÇÃO DE DESASTRES (INTRODUÇÃO)

As cargas de ransomware bloqueiam criptograficamente o armazenamento do sistema, exigindo pagamentos em criptomoedas pelas chaves de desencriptação. A mitigação desta ameaça passa por regras de isolamento de rede, análise de malware em sandbox e cópias de segurança frias isoladas da rede (air-gapped) robustas.

LÊ CADA PONTO DE CONTROLO COM ATENÇÃO E ESCOLHE OU ESCREVE A RESPOSTA CORRETA.

Ponto de controlo 1: Desafio de escolha múltipla

1. Qual é o principal mecanismo de um ataque de ransomware?

- A. Encriptação criptográfica dos ficheiros do utilizador para negar o acesso ao sistema
- B. Injetar comandos SQL maliciosos em campos de formulários
- C. Intercetar pacotes de rede numa ligação Wi-Fi pública
- D. Falsificar cabeçalhos de e-mail para contornar a validação SPF

2. O que é uma cópia de segurança offline (a frio)?

- A. Uma cópia de armazenamento desligada da rede para a proteger da propagação de software malicioso
- B. Uma cópia de segurança guardada no disco rígido do servidor web principal
- C. Uma cache temporária de registos do registo do sistema
- D. Uma ferramenta administrativa usada para repor palavras-passe de utilizadores

3. Como devem as equipas de segurança isolar os sistemas infetados durante um ataque de ransomware?

- A. Desligar imediatamente os cabos de rede e desativar as interfaces sem fios
- B. Atualizar a base de dados de assinaturas do antivírus
- C. Desligar o servidor DNS principal
- D. Mudar o nome das extensões dos ficheiros comprometidos

4. Porque é que as agências de segurança desaconselham pagar os resgates do ransomware?

- A. Pagar incentiva os atacantes e não garante a entrega da chave de desencriptação
- B. Invalida automaticamente todas as apólices de seguro da empresa
- C. Notifica automaticamente todos os clientes por e-mail
- D. Corrompe os restantes ficheiros de cópia de segurança do sistema

5. O que é um plano de recuperação de desastres (DRP)?

- A. Um processo estruturado para restabelecer as operações e os dados após um comprometimento do sistema
- B. Uma configuração de firewall que mapeia portas de rede de entrada
- C. Um esquema de base de dados que lista os privilégios administrativos dos utilizadores
- D. Um protocolo de autenticação de e-mail que rejeita domínios falsificados

Ponto de controlo 2: Desafio de verdadeiro ou falso

6 Pergunta 6

6. As cargas de ransomware podem propagar-se facilmente para cópias de segurança online ligadas à rede.

○ Verdadeiro ○ Falso

7 Pergunta 7

7. Pagar o resgate em criptomoeda garante que os ficheiros serão decifrados com êxito.

○ Verdadeiro ○ Falso

8 Pergunta 8

8. Desligar da rede os sistemas infetados ajuda a impedir que o ransomware se espalhe para sistemas adjacentes.

○ Verdadeiro ○ Falso

9 Pergunta 9

9. A criptografia simétrica nunca é usada pelo ransomware para encriptar o armazenamento do sistema.

○ Verdadeiro ○ Falso

10 Pergunta 10

10. Testar regularmente os procedimentos de restauro de dados é uma parte essencial da recuperação de desastres.

○ Verdadeiro ○ Falso

Ponto de controlo 3: Inserção de termos-chave

Lê cada frase abaixo e preenche o espaço em branco com o termo correto do banco de palavras.

1. Impedir o acesso a ficheiros locais recorre à _____ criptográfica.
2. O código malicioso ativo executado num sistema é a _____ .
3. As cópias de armazenamento externas e desligadas da rede constituem uma _____ segura.
4. Impedir a propagação do malware exige o _____ de rede dos terminais.
5. O pagamento em criptomoeda exigido pelos cibercriminosos é o _____ .
6. Restaurar os ficheiros de dados operacionais representa a _____ de desastres.

BANCO DE PALAVRAS DE VOCABULÁRIO

CARGA MALICIOSA | CÓPIA OFFLINE | DESASTRE | ENCRIPTAÇÃO | ISOLAMENTO | RECUPERAÇÃO | RESGATE | TROIANO

Escreve aqui as tuas respostas:

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

Ponto de controlo 4: Associação de conceitos de segurança

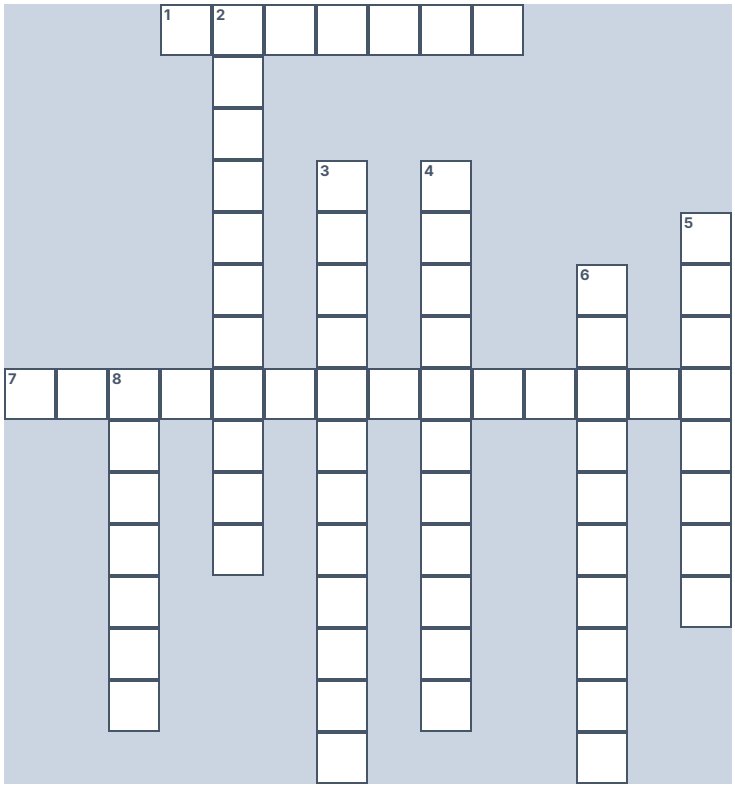
ASSOCIAÇÃO DE DEFINIÇÕES

Associa cada termo de vocabulário da esquerda à sua definição correta da direita, escrevendo a letra correspondente (A-H) na caixa de preenchimento.

☐	1. ENCRIPTAÇÃO	A	Desligar os sistemas de rede infetados.
☐	2. CARGA ÚTIL	B	Ficheiro malicioso disfarçado de ficheiro limpo.
☐	3. CÓPIA DE SEGURANÇA A FRIO	C	Bloquear ficheiros com criptografia.
☐	4. ISOLAMENTO	D	Grande evento de rutura do sistema.
☐	5. RESGATE	E	Executar software malicioso.
☐	6. RECUPERAÇÃO	F	Cópia offline desligada.
☐	7. DESASTRE	G	Restaurar a base de dados a partir da cópia de segurança.
☐	8. CAVALO DE TROIA	H	Pedido de pagamento de chave criptográfica.

Ponto de controlo 5: Palavras cruzadas

Resolve as palavras cruzadas escrevendo letras nas caixas brancas ativas. Os números correspondem às pistas abaixo.



HORIZONTAIS

1. Ficheiro malicioso disfarçado de limpo. (7)

7. Execução de software malicioso. (14)

VERTICAIS

2. Restaurar a base de dados a partir de uma cópia de segurança. (11)

3. Cópia desligada da rede. (12)

4. Bloquear ficheiros por meios criptográficos. (11)

5. Evento de grande perturbação do sistema. (8)

6. Desligar os sistemas de rede infetados. (10)

8. Pedido de pagamento pela chave criptográfica. (7)

Ponto de controlo 5, alternativa: Pistas acessíveis das palavras cruzadas

Os utilizadores de leitores de ecrã e de teclado podem escrever as respostas das palavras cruzadas diretamente nos campos de texto abaixo.

HORIZONTAIS

1 horizontal: Ficheiro malicioso disfarçado de limpo. (7 letras):

7 horizontal: Execução de software malicioso. (14 letras):

VERTICAIS

2 vertical: Restaurar a base de dados a partir de uma cópia de segurança. (11 letras):

3 vertical: Cópia desligada da rede. (12 letras):

4 vertical: Bloquear ficheiros por meios criptográficos. (11 letras):

5 vertical: Evento de grande perturbação do sistema. (8 letras):

6 vertical: Desligar os sistemas de rede infetados. (10 letras):

8 vertical: Pedido de pagamento pela chave criptográfica. (7 letras):

Ponto de controlo 6: Sopa de letras

Encontra os 8 termos-chave de vocabulário escondidos na grelha abaixo. As palavras podem estar na horizontal, na vertical ou na diagonal.

E N C R I P T A C A O U K R B
N X O T N E M A L O S I Z T R
I Y M R Q X I P D A D J R E Q
L V W W L J H T H G B O S E I
F K T S V R Z E H E I G S C A
F L Q C Z M K V R A A U A S W
O J M M H H N H N T R F K T L
A R W H B U F O E Y O Y W S H
I T X A P U N N Z O I Q T I P
P V U O E R T S A S E D U U K
O C A R G A M A L I C I O S A
C A E P M K A N V G G P Q X Y
J K R E C U P E R A C A O V J
Y W Y P J I Z I J N A E I A S
A J F W E K Z K E K Q N J A F

LISTA DE PALAVRAS DE VOCABULÁRIO

ENCRIPTACAO CARGAMALICIOSA COPIAOFFLINE ISOLAMENTO RESGATE
RECUPERACAO DESASTRE TROIANO

Ponto de controlo 6, alternativa: Associação acessível de vocabulário

Associa cada um dos 8 termos de vocabulário da sopa de letras à sua definição correta, escrevendo a letra (A-H) no espaço em branco.

TERMOS DE VOCABULÁRIO

- **A. ENCRIPTACAO**
- **B. CARGAMALICIOSA**
- **C. COPIAOFFLINE**
- **D. ISOLAMENTO**
- **E. RESGATE**
- **F. RECUPERACAO**
- **G. DESASTRE**
- **H. TROIANO**

DEFINIÇÕES E CAMPOS DE ASSOCIAÇÃO

1. Cópia desligada da rede.
2. Ficheiro malicioso disfarçado de limpo.
3. Bloquear ficheiros por meios criptográficos.
4. Pedido de pagamento pela chave criptográfica.
5. Desligar os sistemas de rede infetados.
6. Evento de grande perturbação do sistema.
7. Execução de software malicioso.
8. Restaurar a base de dados a partir de uma cópia de segurança.

Ponto de controlo 7: Desafio de palavras baralhadas

Desembaralha as letras abaixo para revelar conceitos e termos essenciais de cibersegurança. Escreve as tuas respostas nas caixas de resposta fornecidas.

1. ITANPAECCOR
2. EOAOCINPFLFI
3. GRAESTE
4. ARETSDES
5. CROALIAAMIACSG
6. TALENISMOO
7. APREROCACEU
8. RIOTNAO

Atividade bónus: Pensa rápido

3 RESPOSTAS POR CATEGORIA. GANHA QUEM COMPLETAR PRIMEIRO A LISTA.

1	Informações que nunca deves partilhar			
2	Dispositivos que podem ser hackeados			
3	Razões para não pagar um resgate			
4	Hábitos seguros que podes começar hoje			
5	Ferramentas de segurança que conheces			
6	Formas de proteger as tuas contas			
7	Sinais de que um computador está infetado			
8	Locais onde guardar uma cópia de segurança			
9	Ficheiros que nunca queres perder			
10	Formas como o ransomware se espalha			
11	Coisas a fazer na primeira hora de um ataque			
12	Pessoas a contactar durante um ataque			
13	Coisas que o ransomware pode bloquear			
14	Palavras relacionadas com cibersegurança			
15	Organizações que são frequentemente alvo de ataques			

Ponto de controlo 8: Estudos de caso de cibersegurança

Aplica os conceitos que aprendeste para resolver os cenários reais abaixo.

ESTUDO DE CASO 1: CONTENÇÃO DE CARGA DE RANSOMWARE EMPRESARIAL

👷

Cenário: Uma rede local empresarial foi comprometida por ransomware ativo. Os servidores de ficheiros principais começaram a mostrar ficheiros com a extensão .locked.

Questão para debate: Detalha os passos de contenção e descreve o protocolo de recuperação de dados.

ESTUDO DE CASO 2: AVALIAR ARQUITETURAS DE CÓPIAS DE SEGURANÇA OFFLINE

👷

Cenário: Uma empresa quer criar uma estratégia de cópia de segurança de dados que reduza o risco de as cópias serem comprometidas, mesmo que a rede local principal seja totalmente sequestrada por ransomware.

Questão para debate: Concebe um sistema seguro de cofre de armazenamento de cópias de segurança offline.

Ponto de controlo 9: Decifrar o código

Um profissional de cibersegurança protege os ativos de rede contra agentes de ameaça online. Usa a chave Letra-Número abaixo para decifrar a mensagem, escrevendo as letras correspondentes nos espaços em branco.

CHAVE DE ENCRIPTAÇÃO DE LETRAS PARA NÚMEROS

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26



Mensagem decifrada:

DICA: CADA NÚMERO REPRESENTA A POSIÇÃO DESSA LETRA NO ALFABETO (P. EX., 1 = A, 2 = B, 26 = Z).

Ponto de controlo 10: Perguntas frequentes básicas sobre cibersegurança (Parte A)

Revê perguntas e respostas comuns sobre a mitigação de ameaças online.

Q1: O que é ransomware?

O ransomware é software malicioso concebido para bloquear o acesso a sistemas informáticos ou ficheiros até ser pago um resgate.

Q2: Como se propaga o ransomware?

Através de anexos de e-mails de phishing, vulnerabilidades de software sem correções e sistemas de acesso remoto comprometidos. [1]

Q3: Porque é que o pagamento é pedido em criptomoedas?

As criptomoedas como o Bitcoin oferecem um anonimato relativo, dificultando o rastreio dos fundos pelas autoridades policiais.

Q4: O antivírus bloqueia ransomware?

Sim, mas o antivírus baseado em assinaturas pode falhar contra cargas de ransomware zero-day recém-criadas.

Q5: O que é uma cópia de segurança isolada da rede (air-gapped)?

Uma cópia de segurança sem ligação física ou lógica à rede principal, o que a protege contra a propagação.

Ponto de controlo 10: Perguntas frequentes básicas sobre cibersegurança (Parte B)

Revê perguntas e respostas comuns sobre a mitigação de ameaças online.

Q6: O que é a dupla extorsão?

Quando os atacantes não só encriptam ficheiros como também roubam dados sensíveis para ameaçar divulgá-los publicamente se não forem pagos.

Q7: O que é um desencriptador?

Um utilitário de software que contém a chave criptográfica necessária para restaurar ficheiros bloqueados em texto simples.

Q8: Como se deteta ransomware precocemente?

Monitorizando os sistemas de ficheiros para detetar atividade súbita e maciça de modificação e mudança de nome de ficheiros.

Q9: Qual é o papel do seguro?

O seguro de cibersegurança pode ajudar a cobrir os custos de recuperação, mas as condições de cobertura e as regras sobre o pagamento de resgates variam consoante a apólice.

Q10: Devo reiniciar um sistema infetado?

Não, reiniciar pode destruir as provas da memória volátil; isola-o antes da rede. [1]

Ponto de controlo 10: Perguntas frequentes avançadas sobre segurança (Parte C)

Explora aspetos técnicos avançados das estruturas de segurança, da análise de malware e da conformidade de dados.

Q1: Como usa o ransomware a encriptação assimétrica?

Utiliza uma chave pública incorporada no software malicioso para encriptar ficheiros, exigindo a chave privada do atacante para os desencriptar.

Q2: Porque é que também se utiliza encriptação simétrica?

A encriptação simétrica (como o AES) é rápida e pode bloquear bases de dados enormes em minutos, enquanto as chaves assimétricas protegem a chave AES.

Q3: O que é a segmentação lógica?

Dividir as redes em zonas isoladas, impedindo que o malware se propague lateralmente dos postos de trabalho para os servidores principais.

Q4: O que é o armazenamento WORM?

Suportes Write-Once, Read-Many, que impedem que os dados de cópia de segurança sejam editados, substituídos ou eliminados por cargas de ransomware.

Q5: O que são cópias de sombra (shadow copies)?

Cópias de segurança locais criadas pelo Windows; o ransomware costuma eliminá-las primeiro, recorrendo a ferramentas administrativas.

Ponto de controlo 10: Perguntas frequentes avançadas sobre segurança (Parte D)

Explora aspetos técnicos avançados das estruturas de segurança, da análise de malware e da conformidade de dados.

Q6: Como possibilita o roubo de credenciais o ransomware?

Os atacantes compram credenciais de administrador divulgadas para iniciar sessão através de ambientes de trabalho remotos e executar manualmente ransomware em toda a rede.

Q7: O que são testes de restauro simulado (dry-run)?

Restaurar regularmente cópias de segurança de bases de dados em ambientes de teste isolados para verificar se a velocidade de restauro e a integridade dos dados cumprem as métricas de recuperação de desastres.

Q8: Como impede a deteção em terminais (EDR) o ransomware?

Analisando o comportamento dos processos (por exemplo, a encriptação rápida) e suspendendo rapidamente a aplicação suspeita.

Q9: O que é um modelo de ransomware como serviço (RaaS)?

Um modelo de franquia em que os programadores de software malicioso alugam construtores de ransomware a afiliados em troca de uma percentagem dos pagamentos.

Q10: Como é que um RDP sem atualizações desencadeia ransomware?

Gateways expostos do Remote Desktop Protocol sem atualizações permitem que os atacantes usem força bruta nos inícios de sessão e executem malware manualmente.

Parte 11: 10 factos e perspetivas do mundo real sobre cibersegurança

Revê factos reais sobre violações de segurança, mecanismos de defesa e normas de conformidade.

1. PERSPETIVA SOBRE SEGURANÇA

Os agentes de ransomware usam frequentemente ferramentas como o vssadmin.exe para eliminar as cópias de sombra do Windows e bloquear restauros locais. [1]

2. PERSPETIVA SOBRE SEGURANÇA

As chaves simétricas AES-256 são normalmente usadas para encriptar o conteúdo dos ficheiros, que são depois bloqueados com chaves públicas RSA.

3. PERSPETIVA SOBRE SEGURANÇA

Recuperar de um ataque de ransomware bem-sucedido pode demorar semanas, e é por isso que as cópias de segurança offline testadas são importantes.

4. PERSPETIVA SOBRE SEGURANÇA

O FBI não apoia o pagamento de um resgate e avisa que pagar não garante que recuperes quaisquer dados. [2]

5. PERSPETIVA SOBRE SEGURANÇA

Os planos de recuperação de desastres (DRP) devem definir um Objetivo de Tempo de Recuperação (RTO) e um Objetivo de Ponto de Recuperação (RPO).

6. PERSPETIVA SOBRE SEGURANÇA

O FBI recomenda cópias de segurança encriptadas e imutáveis, ou seja, que não podem ser alteradas nem eliminadas. [3]

7. PERSPETIVA SOBRE SEGURANÇA

Os programadores de ransomware utilizam técnicas avançadas de ofuscação para contornar os analisadores de antivírus tradicionais baseados em assinaturas.

8. PERSPETIVA SOBRE SEGURANÇA

A segmentação de rede restringe o movimento lateral, ajudando a impedir que o ransomware se propague para além do primeiro anfitrião infetado. [3]

9. PERSPETIVA SOBRE SEGURANÇA

Serviços remotos expostos e mal protegidos, como o Remote Desktop Protocol (RDP), são um ponto de entrada comum do ransomware. [1]

10. PERSPETIVA SOBRE SEGURANÇA

A CISA aconselha a manter cópias de segurança encriptadas offline, uma vez que muitas variantes de ransomware procuram e eliminam as cópias de segurança acessíveis. [1]

Referências técnicas e fontes

O guia de estudo e os puzzles interativos são compilados a partir das normas globais do NIST, da OWASP e de conformidade em matéria de privacidade de dados.

REFERÊNCIAS ACADÉMICAS E DO SETOR

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

[2] FBI Internet Crime Complaint Center. (n.d.). Ransomware.
https://www.ic3.gov/CrimeInfo/Ransomware

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

Soluções: Ponto de controlo 1 - Escolha múltipla

1 Pergunta 1

Resposta correta: A

NOTA PARA O PROFESSOR

Qual é o principal mecanismo de um ataque de ransomware? → Encriptação criptográfica dos ficheiros do utilizador para negar o acesso ao sistema

2 Pergunta 2

Resposta correta: A

NOTA PARA O PROFESSOR

O que é uma cópia de segurança offline (a frio)? → Uma cópia de armazenamento desligada da rede para a proteger da propagação de software malicioso

3 Pergunta 3

Resposta correta: A

NOTA PARA O PROFESSOR

Como devem as equipas de segurança isolar os sistemas infetados durante um ataque de ransomware? → Desligar imediatamente os cabos de rede e desativar as interfaces sem fios

4 Pergunta 4

Resposta correta: A

NOTA PARA O PROFESSOR

Porque é que as agências de segurança desaconselham pagar os resgates do ransomware? → Pagar incentiva os atacantes e não garante a entrega da chave de desencriptação

5 Pergunta 5

Resposta correta: A

NOTA PARA O PROFESSOR

O que é um plano de recuperação de desastres (DRP)? → Um processo estruturado para restabelecer as operações e os dados após um comprometimento do sistema

Soluções: Ponto de controlo 2 - Verdadeiro ou falso

6 Pergunta 6

Resposta correta: Verdadeiro

NOTA PARA O PROFESSOR

As cargas de ransomware podem propagar-se facilmente para cópias de segurança online ligadas à rede.

7 Pergunta 7

Resposta correta: Falso

NOTA PARA O PROFESSOR

Falso: o FBI avisa que pagar não garante que recuperes quaisquer dados. [2]

8 Pergunta 8

Resposta correta: Verdadeiro

NOTA PARA O PROFESSOR

Verdadeiro: a CISA aconselha desligar os anfitriões infetados ou colocar a rede offline para conter a propagação.

9 Pergunta 9

Resposta correta: Falso

NOTA PARA O PROFESSOR

Falso: o ransomware normalmente encripta ficheiros com cifras simétricas rápidas, como o AES.

10 Pergunta 10

Resposta correta: Verdadeiro

NOTA PARA O PROFESSOR

Testar regularmente os procedimentos de restauro de dados é uma parte essencial da recuperação de desastres.

Soluções de vocabulário e grelha de avaliação

Grelha de classificação do professor: atribui 1 ponto por cada correspondência correta (8 pontos no total) e por cada termo de contexto (6 pontos no total).

PONTO DE CONTROLO 4: SOLUÇÕES – ASSOCIAÇÃO DE CONCEITOS

C 1. ENCRIPTAÇÃO	E 2. CARGA ÚTIL	F 3. CÓPIA DE SEGURANÇA A FRIO	A 4. ISOLAMENTO
H 5. RESGATE	G 6. RECUPERAÇÃO	D 7. DESASTRE	B 8. CAVALO DE TROIA

PONTO DE CONTROLO 3: SOLUÇÕES – TERMOS-CHAVE

1 ENCRIPTAÇÃO	2 CARGA MALICIOSA	3 CÓPIA OFFLINE	4 ISOLAMENTO
5 RESGATE	6 RECUPERAÇÃO		

PONTO DE CONTROLO 6, ALTERNATIVA: SOLUÇÕES – ASSOCIAÇÃO DE PALAVRAS

1 C – COPIAOFFLINE	2 H – TROIANO	3 A – ENCRIPTACAO	4 E – RESGATE
5 D – ISOLAMENTO	6 G – DESASTRE	7 B – CARGAMALICIOSA	8 F – RECUPERACAO

NOTAS DE DEBATE PARA PROFESSORES

Termos-chave:
Verifica se os alunos sabem explicar ENCRIPTAÇÃO, CARGA ÚTIL e CÓPIA DE SEGURANÇA A FRIO por palavras suas e dar um exemplo de cada.

Estudos de caso:
Pede aos alunos que justifiquem as recomendações com factos da ficha e não com suposições.

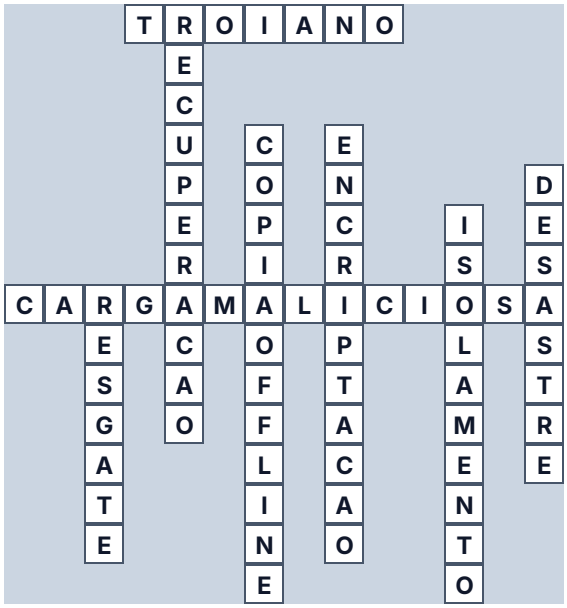
Avaliação das fontes:
Pede aos alunos que confirmem pelo menos uma afirmação nas fontes da ficha e discutam porque é que números, preços e regras podem mudar com o tempo.

Soluções dos puzzles e notas para o professor

SOLUÇÃO DO CAÇA-PALAVRAS



SOLUÇÃO DAS PALAVRAS CRUZADAS



GUIA DO PROFESSOR PARA AS SOLUÇÕES DAS PALAVRAS CRUZADAS

HORIZONTAIS

1 horizontal: TROIANO Ficheiro malicioso disfarçado de limpo. (7 letras)

7 horizontal: CARGAMALICIOSA Execução de software malicioso. (14 letras)

VERTICAIS

2 vertical: RECUPERACAO Restaurar a base de dados a partir de uma cópia de segurança. (11 letras)

3 vertical: COPIAOFFLINE Cópia desligada da rede. (12 letras)

4 vertical: ENCRIPTACAO Bloquear ficheiros por meios criptográficos. (11 letras)

5 vertical: DESASTRE Evento de grande perturbação do sistema. (8 letras)

6 vertical: ISOLAMENTO Desligar os sistemas de rede infetados. (10 letras)

8 vertical: RESGATE Pedido de pagamento pela chave criptográfica. (7 letras)

Palavras baralhadas e soluções da cifra

Chave de correção da atividade de reordenação de letras do vocabulário e do Desafio do Código Secreto.

CHAVE DE SOLUÇÕES DAS PALAVRAS EMBARALHADAS

1.	ITANPAECCOR	ENCRIPTACAO	5.	CROALIAAMIACSG	CARGAMALICIOSA
2.	EOAOCINPFLFI	COPIAOFFLINE	6.	TALENISMOO	ISOLAMENTO
3.	GRAESTE	RESGATE	7.	APRERO CACEU	RECUPERACAO
4.	ARETSDES	DESASTRE	8.	RIOTNAO	TROIANO

CHAVE DO DESAFIO DO CÓDIGO SECRETO

"RESTAURA DADOS ENCRIPTADOS COM A COPIA OFFLINE"

Soluções dos estudos de caso

A Estudo de caso 1: Contenção de carga de ransomware empresarial

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise do cenário: A rede local de uma empresa foi violada por ransomware ativo. Os principais servidores de ficheiros começaram a mostrar ficheiros com a extensão .locked.
- Estratégia e solução recomendadas: Desligar da rede local todos os servidores afetados. Terminar as sessões administrativas ativas. Restaurar os ficheiros não comprometidos a partir de um sistema de cópia de segurança offline seguro, com proteção contra escrita.

B Estudo de caso 2: Avaliar arquiteturas de cópias de segurança offline

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise de cenário: Uma empresa pretende conceber uma estratégia de cópias de segurança que reduza o risco de estas serem comprometidas, mesmo que a rede local principal seja totalmente sequestrada por ransomware.
- Estratégia e solução recomendadas: Implementar armazenamento WORM (write-once-read-many). Criar um air-gap lógico desligando o sistema de cópias de segurança de todas as redes e aplicar a rotação diária de suportes físicos.