Naam: _____ Datum: _____ Score: _____

Ransomware-aanvallen en zakelijk Herstel

Uitvoering van de payload, cryptografische bestandsversleuteling, offline back-ups, indammingsprocedures en noodherstel.

LEEROVERZICHT: RANSOMWAREAANVALLEN

BEVEILIGD

GEGEVENSVERSLEUTELING

256-bits AES-standaard

COMPLIANT

WERELDWIJDE NORMEN

AVG- en CCPA-kaders

ZERO-TRUST

TOEGANGSBELEID

Multifactorauthenticatie

Welkom! Dit activiteitenpakket leidt je door ransomware-aanvallen en bedrijfsherstel. Je verkent het uitvoeren van payloads, bestandsversleuteling, offline back-ups, het beheersen van bedreigingen, betalingen in cryptovaluta en rampenherstelplannen.

CONTROLEPUNTEN VAN HET WERKBLAD

- [ ] **Deel 1-4: Beheers cyberbeveiliging en dreigingspreventie.**
- [ ] **Deel 5-7: Los kruiswoord- en woordzoekpuzzels op.**
- [ ] **Deel 8-9: Los casestudy's en de codeopdracht op.**
- [ ] **Deel 10: Bekijk de pagina's met veelgestelde vragen (basis en gevorderd).**
- [ ] **Deel 11: Ontdek 10 interessante feiten uit de praktijk.**
- [ ] **Bonus: Snel denken-uitdaging.**

Open de VPN.com-gids over cyberbeveiliging

URL: https://www.vpn.com/nl/cyberbeveiliging/ransomware-aanval/

Jouw leertraject: herstel na ransomware

- Maak onderscheid tussen trojan-, ransomware- en spyware-payloads.
- Analyseer schadelijke bestanden in beveiligde sandboxomgevingen.
- Procedures opstellen voor snelle netwerkisolatie en insluiting.

INSTRUCTIES: GIDS OVER RANSOMWAREAANVALLEN

Beantwoord de meerkeuzevragen en de vragen waar/onwaar, vul de zinnen aan met behulp van de woordenbank, koppel de definities en los de kruiswoordpuzzel en de woordzoeker op. Pas je kennis toe op herstel na ransomware. Sluit af met de bonusopdracht Snel denken.

RANSOMWAREAANVALLEN EN HERSTEL NA EEN RAMP (INLEIDING)

Ransomware-payloads vergrendelen de systeemopslag cryptografisch en eisen betalingen in cryptovaluta voor ontsleutelingssleutels. Deze dreiging beperk je met netwerkisolatieregels, malware-analyse in een sandbox en robuuste air-gapped cold back-ups.

LEES ELK CONTROLEPUNT ZORGVULDIG EN KIES OF SCHRIJF HET JUISTE ANTWOORD.

Controlepunt 1: Meerkeuzeopdracht

1. Wat is het belangrijkste mechanisme van een ransomware-aanval?

- A. Cryptografische versleuteling van gebruikersbestanden om de toegang tot het systeem te ontzeggen
- B. Schadelijke SQL-opdrachten in formuliervelden injecteren
- C. Netwerkpakketten snuffelen op een openbare wifiverbinding
- D. E-mailheaders vervalsen om SPF-validatie te omzeilen

2. Wat is een offline (cold) back-up?

- A. Een opslagkopie die van het netwerk is losgekoppeld om haar te beschermen tegen de verspreiding van malware
- B. Een back-up die op de harde schijf van de primaire webserver wordt opgeslagen
- C. Een tijdelijke cache van logs van het systeemregister
- D. Een beheertool om gebruikerswachtwoorden te resetten

3. Hoe moeten beveiligingsteams geïnfecteerde systemen isoleren tijdens een ransomware-aanval?

- A. Netwerkkabels loskoppelen en draadloze interfaces onmiddellijk uitschakelen
- B. De database met antivirushandtekeningen bijwerken
- C. De primaire DNS-server uitschakelen
- D. De bestandsextensies van de aangetaste bestanden hernoemen

4. Waarom raden beveiligingsdiensten af om op ransomware-eisen in te gaan?

- A. Betalen moedigt aanvallers aan en garandeert niet dat de ontsleutelingssleutel wordt geleverd
- B. Het maakt automatisch alle bedrijfsverzekeringen ongeldig
- C. Het stuurt automatisch elke klant een e-mail
- D. Het beschadigt de resterende back-upbestanden van het systeem

5. Wat is een noodherstelplan (DRP)?

- A. Een gestructureerd proces om de werking en gegevens te herstellen nadat een systeem is gecompromitteerd
- B. Een firewallconfiguratie die inkomende netwerkpoorten in kaart brengt
- C. Een databaseschema met de beheerdersrechten van gebruikers
- D. Een e-mailauthenticatieprotocol dat vervalste domeinen weigert

Controlepunt 2: Waar-of-onwaar-opdracht

6 Vraag 6

6. Ransomware-payloads kunnen zich gemakkelijk verspreiden naar online back-ups die met het netwerk zijn verbonden.

- ◯ Waar
- ◯ Onwaar

7 Vraag 7

7. Het betalen van het losgeld in cryptovaluta garandeert dat bestanden met succes worden ontsleuteld.

- ◯ Waar
- ◯ Onwaar

8 Vraag 8

8. Het loskoppelen van geïnfecteerde systemen van het netwerk helpt te voorkomen dat ransomware zich naar aangrenzende systemen verspreidt.

- ◯ Waar
- ◯ Onwaar

9 Vraag 9

9. Symmetrische cryptografie wordt door ransomware nooit gebruikt om systeemopslag te versleutelen.

- ◯ Waar
- ◯ Onwaar

10 Vraag 10

10. Het regelmatig testen van procedures voor gegevensherstel is een cruciaal onderdeel van rampherstel.

- ◯ Waar
- ◯ Onwaar

Controlepunt 3: Kernbegrippen invullen

Lees elke zin hieronder en vul de open plek in met de juiste term uit de woordenbank.

1. Het blokkeren van toegang tot lokale bestanden gebeurt met cryptografische _____ .

2. De actieve kwaadaardige code die op een systeem wordt uitgevoerd, is de _____ .

3. Losgekoppelde opslagkopieën op een andere locatie vormen een veilige _____ .

4. Het stoppen van de verspreiding van malware vereist _____ van endpoints in het netwerk.

5. De cryptovaluta-betaling die cybercriminelen eisen, is het _____ .

6. Het terugzetten van operationele databestanden is onderdeel van het _____ na een calamiteit.

WOORDENBANK

CALAMITEIT HERSTEL ISOLATIE LOSGELD OFFLINE-BACKUP PAYLOAD PHISHING VERSLEUTELING

Schrijf hier je antwoorden:

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

Controlepunt 4: Beveiligingsbegrippen koppelen

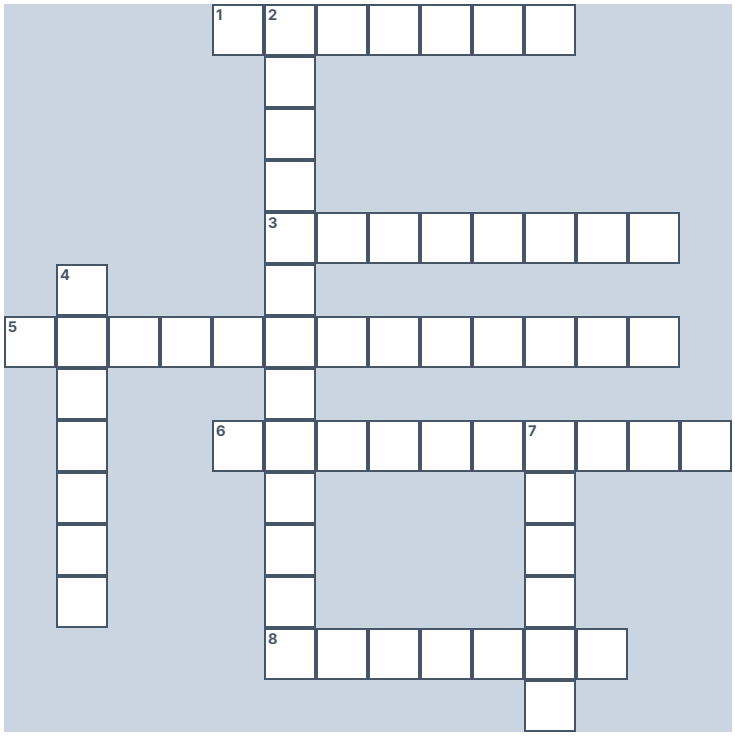
DEFINITIES KOPPELEN

Koppel elke term aan de linkerkant aan de juiste definitie aan de rechterkant door de bijbehorende letter (A-H) in het invulvak te schrijven.

☐	1. VERSLEUTELING	A	Geïnfecteerde netwerksystemen loskoppelen.
☐	2. PAYLOAD	B	Kwaadaardig bestand dat zich voordoet als schoon.
☐	3. KOUDE BACK-UP	C	Bestanden cryptografisch vergrendelen.
☐	4. ISOLATIE	D	Ernstige systeemverstoring.
☐	5. LOSGELD	E	Schadelijke software uitvoeren.
☐	6. HERSTEL	F	Losgekoppelde offlinekopie.
☐	7. RAMP	G	Database herstellen vanaf back-up.
☐	8. TROJAN	H	Verzoek om uitbetaling van een cryptografische sleutel.

Controlepunt 5: Kruiswoordpuzzel

Los de kruiswoordpuzzel op door letters in de actieve witte vakjes te typen. De nummers komen overeen met de aanwijzingen hieronder.



HORIZONTAAL

1. Verzoek tot betaling voor een cryptografische sleutel. (7)

3. Geïnfecteerde netwerksystemen loskoppelen. (8)

5. Bestanden cryptografisch vergrendelen. (13)

6. Ernstige verstoring van systemen. (10)

8. Kwaadaardige software uitvoeren. (7)

VERTICAAL

2. Losgekoppelde offlinekopie. (13)

4. Een database herstellen vanuit een back-up. (7)

7. Kwaadaardig bestand dat zich voordoet als schoon. (6)

Controlepunt 5, alternatief: Toegankelijke kruiswoordaanwijzingen

Gebruikers van schermlezers en toetsenborden kunnen de antwoorden van de kruiswoordpuzzel rechtstreeks typen in de tekstvelden hieronder.

HORIZONTAAL

1 horizontaal: Verzoek tot betaling voor een cryptografische sleutel. (7 letters):

3 horizontaal: Geïnfecteerde netwerksystemen loskoppelen. (8 letters):

5 horizontaal: Bestanden cryptografisch vergrendelen. (13 letters):

6 horizontaal: Ernstige verstoring van systemen. (10 letters):

8 horizontaal: Kwaadaardige software uitvoeren. (7 letters):

VERTICAAL

2 verticaal: Losgekoppelde offlinekopie. (13 letters):

4 verticaal: Een database herstellen vanuit een back-up. (7 letters):

7 verticaal: Kwaadaardig bestand dat zich voordoet als schoon. (6 letters):

Controlepunt 6: Verborgen woorden zoeken

Zoek de 8 belangrijkste vakwoorden die in het onderstaande rooster verborgen zijn. Woorden kunnen horizontaal, verticaal of diagonaal staan.

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

WOORDENLIJST

VERSLEUTELING PAYLOAD OFFLINEBACKUP ISOLATIE LOSGELD HERSTEL CALAMITEIT TROJAN

Controlepunt 6, alternatief: Toegankelijk woordenschat koppelen

Koppel elk van de 8 vaktermen uit de woordzoeker aan de juiste definitie door de letter (A-H) in de lege ruimte te schrijven.

BEGRIPPEN

- **A. VERSLEUTELING**
- **B. PAYLOAD**
- **C. OFFLINEBACKUP**
- **D. ISOLATIE**
- **E. LOSGELD**
- **F. HERSTEL**
- **G. CALAMITEIT**
- **H. TROJAN**

DEFINITIES EN KOPPELVELDEN

1. Losgekoppelde offlinekopie.
2. Kwaadaardig bestand dat zich voordoet als schoon.
3. Bestanden cryptografisch vergrendelen.
4. Verzoek tot betaling voor een cryptografische sleutel.
5. Geïnfecteerde netwerksystemen loskoppelen.
6. Ernstige verstoring van systemen.
7. Kwaadaardige software uitvoeren.
8. Een database herstellen vanuit een back-up.

Controlepunt 7: Opdracht met door elkaar gehaalde woorden

Ontcijfer de letters hieronder om kernbegrippen van cyberbeveiliging te onthullen. Schrijf je antwoorden in de invulvelden.

1. URENEETLVIG LS
2. UIFNFOKEPA CBL
3. GLEDSLO
4. IIMTAETCAL
5. ODLYPAA
6. IELTIASO
7. HETLESR
8. ONTAJR

Bonusopdracht: Snel denken

3 ANTWOORDEN PER CATEGORIE. WIE DE LIJST ALS EERSTE INVULT, WINT.

1	Informatie die je nooit zou moeten delen			
2	Apparaten die gehackt kunnen worden			
3	Redenen om geen losgeld te betalen			
4	Veilige gewoonten die je vandaag kunt beginnen			
5	Beveiligingstools die je kent			
6	Manieren om je accounts te beschermen			
7	Tekenen dat een computer is geïnfecteerd			
8	Plekken om een back-up te bewaren			
9	Bestanden die je nooit wilt kwijtraken			
10	Manieren waarop ransomware zich verspreidt			
11	Dingen die je doet in het eerste uur van een aanval			
12	Mensen die je tijdens een aanval kunt bellen			
13	Dingen die ransomware kan vergrendelen			
14	Woorden die met cyberbeveiliging te maken hebben			
15	Organisaties die vaak doelwit zijn			

Controlepunt 8: Casestudy's cyberbeveiliging

Pas de concepten die je hebt geleerd toe om de onderstaande praktijkscenario's op te lossen.

CASESTUDY 1: INDAMMEN VAN EEN RANSOMWARE-PAYLOAD IN EEN ENTERPRISE-OMGEVING



Scenario: Een lokaal bedrijfsnetwerk is aangetast door actieve ransomware. Belangrijke bestandsservers zijn begonnen bestandsextensies met .locked te tonen.

Discussievraag: Beschrijf in detail de stappen voor indamming en schets het protocol voor gegevensherstel.

CASESTUDY 2: OFFLINE BACK-UPARCHITECTUREN BEOORDELEN



Scenario: Een onderneming wil een strategie voor gegevensback-ups ontwerpen die het risico verkleint dat back-ups worden gecompromitteerd, zelfs als het primaire lokale netwerk volledig door ransomware wordt gekaapt.

Discussievraag: ontwerp een beveiligd offline kluissysteem voor back-ups.

Controlepunt 9: De code ontcijferen

Een cyberbeveiligingsprofessional beschermt netwerkmiddelen tegen online bedreigers. Gebruik de onderstaande letter-naar-cijfersleutel om het bericht te ontcijferen door de bijbehorende letters in de lege vakjes te schrijven.

LETTER-NAAR-CIJFER-VERSLEUTELINGSSLEUTEL

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

8	5	18	19	20	5	12		22	5	18	19	12	5	21	20	5	12	4	5

4	1	20	1		22	1	14	21	9	20		15	6	6	12	9	14	5

2	1	3	11	21	16

Ontcijferd bericht:

TIP: ELK GETAL STAAT VOOR DE POSITIE VAN DIE LETTER IN HET ALFABET (BIJV. 1 = A, 2 = B, 26 = Z).

Controlepunt 10: Veelgestelde vragen over cyberbeveiliging – basis (Deel A)

Bekijk veelgestelde vragen en antwoorden over het beperken van online dreigingen.

Q1: Wat is ransomware?

Ransomware is schadelijke software die is ontworpen om de toegang tot computersystemen of bestanden te blokkeren totdat een losgeldbedrag is betaald.

Q2: Hoe verspreidt ransomware zich?

Via phishingbijlagen in e-mail, niet-gepatchte softwarekwetsbaarheden en gecompromitteerde systemen voor toegang op afstand. [1]

Q3: Waarom wordt er betaling in cryptovaluta gevraagd?

Cryptovaluta zoals Bitcoin bieden relatieve anonimiteit, waardoor het voor wetshandhavers moeilijk is om de geldstromen te volgen.

Q4: Blokkeert antivirussoftware ransomware?

Ja, maar antivirussoftware op basis van handtekeningen kan falen tegen nieuw gemaakte zero-day-ransomware-payloads.

Q5: Wat is een air-gapped back-up?

Een back-upkopie die geen fysieke of logische verbinding met het primaire netwerk heeft, waardoor ze tegen verspreiding is beschermd.

Controlepunt 10: Veelgestelde vragen over cyberbeveiliging – basis (Deel B)

Bekijk veelgestelde vragen en antwoorden over het beperken van online dreigingen.

Q6: Wat is dubbele afpersing?

Wanneer aanvallers bestanden niet alleen versleutelen maar ook gevoelige gegevens stelen om met openbare lekken te dreigen als er niet wordt betaald.

Q7: Wat is een decryptor?

Een softwarehulpprogramma met de cryptografische sleutel die nodig is om vergrendelde bestanden weer naar leesbare tekst te herstellen.

Q8: Hoe detecteer je ransomware vroegtijdig?

Door bestandssystemen te bewaken op plotselinge, massale bestandswijzigingen en hernoemingen.

Q9: Welke rol speelt verzekering?

Een cyberverzekering kan helpen bij het dekken van herstelkosten, maar de dekkingsvoorwaarden en de regels over losgeldbetalingen verschillen per polis.

Q10: Moet ik een geïnfecteerd systeem opnieuw opstarten?

Nee, opnieuw opstarten kan bewijs in vluchtig geheugen vernietigen; isoleer het apparaat in plaats daarvan van het netwerk. [1]

Controlepunt 10: Veelgestelde vragen over beveiliging – gevorderd (Deel C)

Verken geavanceerde technische aspecten van beveiligingsframeworks, malwareanalyse en gegevenscompliance.

Q1: Hoe gebruikt ransomware asymmetrische versleuteling?

Het gebruikt een in de malware ingebouwde publieke sleutel om bestanden te versleutelen, waarbij de privésleutel van de aanvaller nodig is om ze te ontsleutelen.

Q2: Waarom wordt ook symmetrische versleuteling gebruikt?

Symmetrische versleuteling (zoals AES) is snel en kan enorme databases binnen enkele minuten vergrendelen, terwijl asymmetrische sleutels de AES-sleutel beveiligen.

Q3: Wat is logische segmentatie?

Netwerken opdelen in geïsoleerde zones, zodat malware zich niet lateraal kan verspreiden van werkstations naar kernservers.

Q4: Wat is WORM-opslag?

Write-Once-Read-Many-media, waardoor ransomware-payloads back-upgegevens niet kunnen bewerken, overschrijven of verwijderen.

Q5: Wat zijn schaduwkopieën?

Lokale back-upsnapshots die door Windows worden gemaakt; ransomware verwijdert deze meestal als eerste met beheertools.

Controlepunt 10: Veelgestelde vragen over beveiliging – gevorderd (Deel D)

Verken geavanceerde technische aspecten van beveiligingsframeworks, malwareanalyse en gegevenscompliance.

Q6: Hoe maakt diefstal van inloggegevens ransomware mogelijk?

Aanvallers kopen gelekte beheerdersinlogs om in te loggen via externe bureaubladen en handmatig ransomware uit te voeren in het hele netwerk.

Q7: Wat is een dry-run-test van herstel?

Back-updatabases regelmatig terugzetten in geïsoleerde testomgevingen om te controleren of de herstelsnelheid en de gegevensintegriteit voldoen aan de rampherstelnormen.

Q8: Hoe stopt endpointdetectie (EDR) ransomware?

Door het procesgedrag te analyseren (bijvoorbeeld snelle versleuteling) en de kwaadaardige toepassing snel te onderbreken.

Q9: Wat is een ransomware-as-a-service-model (RaaS)?

Een franchisemodel waarbij malware-ontwikkelaars ransomwarebouwpakketten verhuren aan partners in ruil voor een percentage van de opbrengsten.

Q10: Hoe leidt een niet-gepatchte RDP tot ransomware?

Blootgestelde, niet-gepatchte Remote Desktop Protocol-gateways stellen aanvallers in staat om logins met brute force te kraken en handmatig malware te starten.

Deel 11: 10 cyberbeveiligingsfeiten en inzichten uit de praktijk

Bekijk feiten uit de praktijk over beveiligingsincidenten, verdedigingsmechanismen en compliancenormen.

1. BEVEILIGINGSINZICHT

Ransomware-actoren gebruiken vaak hulpmiddelen zoals vssadmin.exe om schaduwkopieën van Windows te verwijderen en lokaal herstel te blokkeren. [1]

2. BEVEILIGINGSINZICHT

Symmetrische AES-256-sleutels worden doorgaans gebruikt om bestandspayloads te versleutelen, die vervolgens worden vergrendeld met publieke RSA-sleutels.

3. BEVEILIGINGSINZICHT

Herstel na een geslaagde ransomware-aanval kan weken duren, daarom zijn geteste offline back-ups belangrijk.

4. BEVEILIGINGSINZICHT

De FBI is geen voorstander van het betalen van losgeld en waarschuwt dat betalen niet garandeert dat je gegevens terugkrijgt. [2]

5. BEVEILIGINGSINZICHT

Rampenherstelplannen (DRP) moeten een Recovery Time Objective (RTO) en een Recovery Point Objective (RPO) definiëren.

6. BEVEILIGINGSINZICHT

De FBI raadt back-ups aan die versleuteld en onveranderlijk zijn, wat betekent dat ze niet kunnen worden gewijzigd of verwijderd. [3]

7. BEVEILIGINGSINZICHT

Ontwikkelaars van ransomware gebruiken geavanceerde obfuscatietechnieken om traditionele op handtekeningen gebaseerde antivirusscanners te omzeilen.

8. BEVEILIGINGSINZICHT

Netwerksegmentatie beperkt zijwaartse verplaatsing en helpt voorkomen dat ransomware zich buiten de eerste geïnfecteerde host verspreidt. [3]

9. BEVEILIGINGSINZICHT

Blootgestelde, slecht beveiligde diensten op afstand, zoals Remote Desktop Protocol (RDP), vormen een veelvoorkomend toegangspunt voor ransomware. [1]

10. BEVEILIGINGSINZICHT

CISA adviseert versleutelde back-ups offline te bewaren, omdat veel ransomwarevarianten bereikbare back-ups opsporen en verwijderen. [1]

Technische referenties en bronnen

De studiegids en de interactieve puzzels zijn samengesteld uit wereldwijde NIST- en OWASP-standaarden en standaarden voor naleving van gegevensprivacy.

WETENSCHAPPELIJKE EN BRANCHEREFERENTIES

[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

Antwoordsleutel: Controlepunt 1 - Meerkeuze

1 Vraag 1

Juist antwoord: A

DOCENTENNOTITIE

Wat is het belangrijkste mechanisme van een ransomware-aanval? → Cryptografische versleuteling van gebruikersbestanden om de toegang tot het systeem te ontzeggen

2 Vraag 2

Juist antwoord: A

DOCENTENNOTITIE

Wat is een offline (cold) back-up? → Een opslagkopie die van het netwerk is losgekoppeld om haar te beschermen tegen de verspreiding van malware

3 Vraag 3

Juist antwoord: A

DOCENTENNOTITIE

Hoe moeten beveiligingsteams geïnfecteerde systemen isoleren tijdens een ransomware-aanval? → Netwerkkabels loskoppelen en draadloze interfaces onmiddellijk uitschakelen

4 Vraag 4

Juist antwoord: A

DOCENTENNOTITIE

Waarom raden beveiligingsdiensten af om op ransomware-eisen in te gaan? → Betalen moedigt aanvallers aan en garandeert niet dat de ontsleutelingssleutel wordt geleverd

5 Vraag 5

Juist antwoord: A

DOCENTENNOTITIE

Wat is een noodherstelplan (DRP)? → Een gestructureerd proces om de werking en gegevens te herstellen nadat een systeem is gecompromitteerd

Antwoordsleutel: Controlepunt 2 - Waar of onwaar

6 **Vraag 6** — **Juist antwoord: Waar**

DOCENTENNOTITIE

Ransomware-payloads kunnen zich gemakkelijk verspreiden naar online back-ups die met het netwerk zijn verbonden.

7 **Vraag 7** — **Juist antwoord: Onwaar**

DOCENTENNOTITIE

Onwaar: de FBI waarschuwt dat betalen niet garandeert dat je gegevens terugkrijgt. [2]

8 **Vraag 8** — **Juist antwoord: Waar**

DOCENTENNOTITIE

Waar: CISA adviseert geïnfecteerde hosts los te koppelen of het netwerk offline te halen om verspreiding in te perken.

9 **Vraag 9** — **Juist antwoord: Onwaar**

DOCENTENNOTITIE

Onwaar: ransomware versleutelt bestanden meestal met snelle symmetrische versleutelingen zoals AES.

10 **Vraag 10** — **Juist antwoord: Waar**

DOCENTENNOTITIE

Het regelmatig testen van procedures voor gegevensherstel is een cruciaal onderdeel van rampherstel.

Woordenlijstsleutels en beoordelingsrubriek

Beoordelingsrubriek voor docenten: Geef 1 punt voor elke juiste koppeling (totaal 8 punten) en elk juist contextbegrip (totaal 6 punten).

CONTROLEPUNT 4: ANTWOORDEN BEGRIPPEN KOPPELEN

C 1. VERSLEUTELING	E 2. PAYLOAD	F 3. KOUDE BACK-UP	A 4. ISOLATIE
H 5. LOSGELD	G 6. HERSTEL	D 7. RAMP	B 8. TROJAN

CONTROLEPUNT 3: ANTWOORDEN KERNBEGRIPPEN

1 VERSLEUTELING	2 PAYLOAD	3 OFFLINE-BACKUP	4 ISOLATIE
5 LOSGELD	6 HERSTEL		

CONTROLEPUNT 6, ALTERNATIEF: ANTWOORDEN WOORDEN KOPPELEN

1 C – OFFLINEBACKUP	2 H – TROJAN	3 A – VERSLEUTELING	4 E – LOSGELD
5 D – ISOLATIE	6 G – CALAMITEIT	7 B – PAYLOAD	8 F – HERSTEL

DISCUSSIENOTITIES VOOR DOCENTEN

Kernbegrippen:
Controleer of leerlingen VERSLEUTELING, PAYLOAD en KOUDE BACK-UP in eigen woorden kunnen uitleggen en van elk een voorbeeld kunnen geven.

Casestudy's:
Laat leerlingen hun aanbevelingen onderbouwen met feiten uit het werkblad in plaats van met aannames.

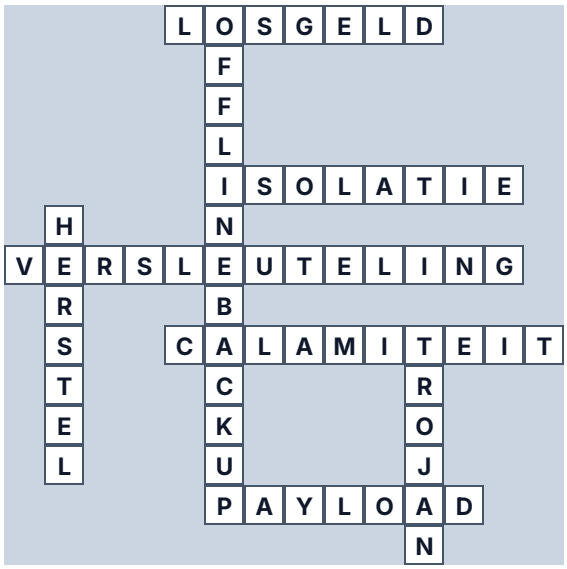
Bronnen beoordelen:
Laat leerlingen ten minste één bewering controleren aan de hand van de bronnen in het werkblad en bespreek waarom cijfers, prijzen en regels kunnen veranderen.

Puzzelsleutels en docentennotities

OPLOSSING WOORDZOEKER

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

OPLOSSING VAN DE KRUISWOORDPUZZEL



DOCENTENGIDS VOOR DE OPLOSSINGEN VAN DE KRUISWOORDPUZZEL

HORIZONTAAL

1 horizontaal: LOSGELD Verzoek tot betaling voor een cryptografische sleutel. (7 letters)

3 horizontaal: ISOLATIE Geïnfecteerde netwerksystemen loskoppelen. (8 letters)

5 horizontaal: VERSLEUTELING Bestanden cryptografisch vergrendelen. (13 letters)

6 horizontaal: CALAMITEIT Ernstige verstoring van systemen. (10 letters)

8 horizontaal: PAYLOAD Kwaadaardige software uitvoeren. (7 letters)

VERTICAAL

2 verticaal: OFFLINEBACKUP Losgekoppelde offlinekopie. (13 letters)

4 verticaal: HERSTEL Een database herstellen vanuit een back-up. (7 letters)

7 verticaal: TROJAN Kwaadaardig bestand dat zich voordoet als schoon. (6 letters)

Sleutel voor husselwoorden en coderaadsel

Beoordelingssleutel voor de woordenschatopdracht met door elkaar gehusselde woorden en de Geheime codeopdracht.

SLEUTEL WOORDEN ORDENEN

1.	URENEETLVIGLS	VERSLEUTELING	5.	ODLYPAA	PAYLOAD
2.	UIFNFOKEPACBL	OFFLINEBACKUP	6.	IELTIASO	ISOLATIE
3.	GLEDSLO	LOSGELD	7.	HETLESR	HERSTEL
4.	IIMTAETCAL	CALAMITEIT	8.	ONTAJR	TROJAN

SLEUTEL VOOR DE GEHEIME CODE-OPDRACHT

"HERSTEL VERSLEUTELDE DATA VANUIT OFFLINE BACKUP"

Antwoordsleutel casestudy's

A Casestudy 1: Indammen van een ransomware-payload in een enterprise-omgeving

Oplossing voor docenten

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Scenarioanalyse: Een lokaal bedrijfsnetwerk is gehackt door actieve ransomware. Belangrijke bestandsservers tonen bestandsextensies met .locked.
- Aanbevolen strategie en oplossing: Koppel alle getroffen servers los van het lokale netwerk. Beëindig actieve beheersessies. Herstel niet-gecompromitteerde bestanden vanuit een beveiligd, tegen schrijven vergrendeld offline back-upsysteem.

B Casestudy 2: Offline back-uparchitecturen beoordelen

Oplossing voor docenten

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Scenarioanalyse: Een groot bedrijf wil een back-upstrategie ontwerpen die het risico verkleint dat back-ups worden gecompromitteerd, zelfs als het primaire lokale netwerk volledig door ransomware wordt gekaapt.
- Aanbevolen strategie en oplossing: Implementeer write-once-read-many-opslag (WORM). Maak een logische air gap door het back-upsysteem van alle netwerken los te koppelen en dwing dagelijkse fysieke rotatie van de media af.