Naam: _____ Datum: _____ Score: _____

Basis van cyberbeveiliging en online dreigingen Preventie

Cyberbeveiligingsdreigingen, netwerkfirewalls, meervoudige authenticatie, beveiligingsraamwerken

LEEROVERZICHT VAN DE BASIS VAN CYBERBEVEILIGING

BEVEILIGD
GEGEVENSVERSLEUTELING
256-bits AES-standaard

COMPLIANT
WERELDWIJDE NORMEN
AVG- en CCPA-kaders

ZERO-TRUST
TOEGANGSBELEID
Multifactorauthenticatie

Welkom! Dit activiteitenpakket leidt je door de basisprincipes van cyberbeveiliging en het voorkomen van online bedreigingen. Je verkent malwarebedreigingen, multifactorauthenticatie, netwerkfirewalls en kaders voor incidentrespons.

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/

Jouw leertraject: basis van cyberbeveiliging

- Veelvoorkomende aanvalsroutes van malware, phishing en inbraak in bedrijfsnetwerken herkennen.
- Voer standaardmaatregelen voor cyberbeveiliging in, waaronder MFA, firewalls en endpointbescherming.
- Beoordeel incidentresponsprocedures om de gevolgen van datalekken te beperken.
- Analyseer organisatorische risicofactoren en beveiligingsafstemming volgens de NIST-richtlijnen.
- Configureer beveiligingsgewoonten om geautomatiseerde credential stuffing te beperken.

INSTRUCTIES VOOR DE GIDS OVER CYBERBEVEILIGING

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 het voorkomen van bedreigingen. Sluit af met de bonusopdracht Snel denken.

BASIS VAN CYBERBEVEILIGING EN DREIGINGSPREVENTIE (INLEIDING)

Cyberbeveiliging beschermt netwerken, systemen en gegevens tegen ongeautoriseerde digitale aanvallen. Het ontwikkelen van stevige beveiligingsgewoonten, het configureren van firewalls, het verplicht stellen van meervoudige authenticatie en het trainen van personeel in het herkennen van dreigingen zijn essentiële onderdelen van de verdediging van een bedrijfsnetwerk.

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

Controlepunt 1: Meerkeuzeopdracht

1. Wat is het belangrijkste doel van een phishingaanval?

- A. Inloggegevens en gevoelige gebruikersgegevens stelen
- B. De zichtbaarheid van een website in zoekmachines verbeteren
- C. De bandbreedtecapaciteit van het netwerk vergroten
- D. Replicatie van back-updatacenters beheren

2. Welk mechanisme biedt de sterkste accountbeveiliging?

- A. Multifactorauthenticatie met hardwaresleutels
- B. Complexe wachtwoorden die elke dertig dagen worden bijgewerkt
- C. Accountinlog beperken tot kantooruren
- D. De gebruikersnaam van het account verbergen in openbare mappen

3. Wat bepaalt de payload van een ransomware-infectie?

- A. Systeembestanden versleutelen en betaling eisen
- B. Stilletjes toetsaanslagen naar externe servers loggen
- C. Ongeautoriseerde advertenties in browsers injecteren
- D. Lokale CPU-resources gebruiken om cryptovaluta te minen

4. Welke invloed heeft een zero-day-exploit op beveiligingsmaatregelen?

- A. Het richt zich op niet-gepatchte, onbekende kwetsbaarheden
- B. Het schakelt automatisch de bedrijfsfirewall uit
- C. Het dwingt het systeem tot een harde herstart
- D. Het vereist geen budget om te herstellen

5. Welk kader regelt beveiligingsmaatregelen binnen bedrijven?

- A. Richtlijnen van het NIST Cybersecurity Framework
- B. Documentschemaspecificaties van W3C HTML5
- C. Handleidingen voor het installeren van printerstuurprogramma's
- D. IETF-definities van routeringsprotocollen

Controlepunt 2: Waar-of-onwaar-opdracht

6 Vraag (waar/onwaar) 6

6. Phishingaanvallen richten zich alleen op persoonlijke e-mailaccounts.

- ◯ Waar
- ◯ Onwaar

7 Vraag (waar/onwaar) 7

7. Multifactorauthenticatie helpt om credential-stuffingaanvallen te blokkeren.

- ◯ Waar
- ◯ Onwaar

8 Vraag (waar/onwaar) 8

8. Firewalls controleren netwerkverkeer om ongeautoriseerde toegang tot poorten te blokkeren.

- ◯ Waar
- ◯ Onwaar

9 Vraag (waar/onwaar) 9

9. Het verhelpen van zero-day-exploits vereist standaardupdates van antivirusdefinities.

- ◯ Waar
- ◯ Onwaar

10 Vraag (waar/onwaar) 10

10. Een honeypot is een lokserver waarmee cybercriminelen worden aangetrokken.

- ◯ Waar
- ◯ Onwaar

Controlepunt 3: Kernbegrippen invullen

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

1. Netwerkbeheerders installeren een _____ om binnenkomend verkeer te filteren.

2. Een aanvaller gebruikt een zero-day- _____ om systeempatches te omzeilen.

3. Aanvallers sturen vervalste e-mails voor _____ -campagnes tegen werknemers.

4. Ransomware is een destructieve vorm van _____ die gebruikersgegevens vergrendelt.

5. Goede wachtwoord- _____ beperkt de risico's van diefstal van inloggegevens.

6. Om gevoelige communicatie te beschermen passen gebruikers protocollen voor _____ toe.

WOORDENBANK

EXPLOIT FIREWALL HONEYPOT HYGIËNE MALWARE MULTIFACTOR PHISHING VERSLEUTELING

Schrijf hier je antwoorden:

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

Controlepunt 4: Beveiligingsbegrippen koppelen

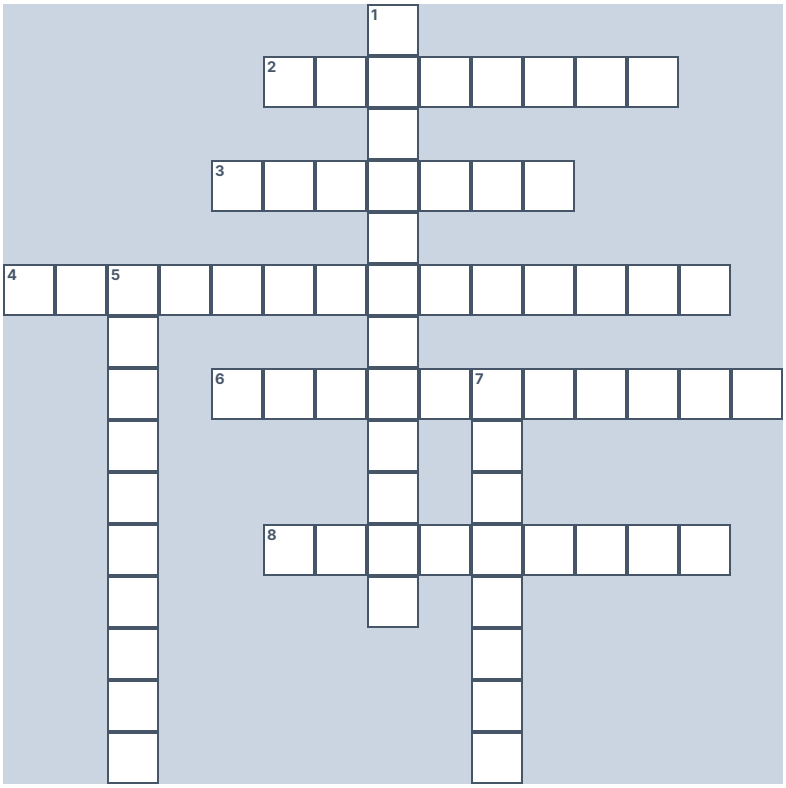
DEFINITIES KOPPELEN

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. Ransomwaredreiging	A	Gestructureerde richtlijnen zoals NIST waarmee cyberrisico's worden beheerd.
☐	2. Multifactorauthenticatie	B	Gestructureerd plan voor het afhandelen en beperken van beveiligingsincidenten.
☐	3. Zero-day-exploit	C	Netwerkbarrière die verkeer filtert op basis van beveiligingsregels.
☐	4. Lokaas-honeypot	D	Malware die gegevens versleutelt en betaling eist voor ontsleuteling.
☐	5. Inbraakfirewall	E	Misbruik van een kwetsbaarheid voordat de leverancier een patch uitbrengt.
☐	6. Incidentrespons	F	Best practices voor het beheren van inloggegevens en authenticatiesleutels.
☐	7. Wachtwoordhygiëne	G	Beveiligingsvalidatie waarvoor twee of meer authenticatiefactoren nodig zijn.
☐	8. Beveiligingsraamwerk	H	Lokaassysteem dat is opgezet om kwaadwillenden aan te trekken en te analyseren.

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

2. Lokvogelsysteem dat is opgezet om kwaadwillenden te lokken en te analyseren (8)

3. Best practices voor het beheren van inloggegevens en authenticatiesleutels (7)

4. Misbruik van een kwetsbaarheid voordat de leverancier een patch uitbrengt (14)

6. Beveiligingsverificatie waarvoor twee of meer authenticatiefactoren nodig zijn (11)

8. Gestructureerde richtlijnen zoals NIST waarmee cyberrisico's worden beheerd (9)

VERTICAAL

1. Gestructureerd plan voor het afhandelen en beperken van beveiligingsincidenten (12)

5. Malware die gegevens versleutelt en financiële betaling eist voor ontsleuteling (10)

7. Netwerkbarrière die verkeer filtert op basis van beveiligingsregels (8)

Controlepunt 5, alternatief: Toegankelijke kruiswoordaanwijzingen

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

HORIZONTAAL

2 horizontaal: Lokvogelsysteem dat is opgezet om kwaadwillenden te lokken en te analyseren (8 letters):

3 horizontaal: Best practices voor het beheren van inloggegevens en authenticatiesleutels (7 letters):

4 horizontaal: Misbruik van een kwetsbaarheid voordat de leverancier een patch uitbrengt (14 letters):

6 horizontaal: Beveiligingsverificatie waarvoor twee of meer authenticatiefactoren nodig zijn (11 letters):

8 horizontaal: Gestructureerde richtlijnen zoals NIST waarmee cyberrisico's worden beheerd (9 letters):

VERTICAAL

1 verticaal: Gestructureerd plan voor het afhandelen en beperken van beveiligingsincidenten (12 letters):

5 verticaal: Malware die gegevens versleutelt en financiële betaling eist voor ontsleuteling (10 letters):

7 verticaal: Netwerkbarrière die verkeer filtert op basis van beveiligingsregels (8 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.

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

WOORDENLIJST

RANSOMWARE MULTIFACTOR ZERODAYEXPLOIT HONEYPOT FIREWALL
INCIDENTPLAN HYGIENE FRAMEWORK

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. RANSOMWARE**
- **B. MULTIFACTOR**
- **C. ZERODAYEXPLOIT**
- **D. HONEYPOT**
- **E. FIREWALL**
- **F. INCIDENTPLAN**
- **G. HYGIENE**
- **H. FRAMEWORK**

DEFINITIES EN KOPPELVELDEN

1. Netwerkbarrière die verkeer filtert op basis van beveiligingsregels.
2. Gestructureerd plan voor het afhandelen en beperken van beveiligingsincidenten.
3. Malware die gegevens versleutelt en financiële betaling eist voor ontsleuteling.
4. Beveiligingsverificatie waarvoor twee of meer authenticatiefactoren nodig zijn.
5. Best practices voor het beheren van inloggegevens en authenticatiesleutels.
6. Gestructureerde richtlijnen zoals NIST waarmee cyberrisico's worden beheerd.
7. Misbruik van een kwetsbaarheid voordat de leverancier een patch uitbrengt.
8. Lokvogelsysteem dat is opgezet om kwaadwillenden te lokken en te analyseren.

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. RWMOARAESN
2. DEARYIZOETPLXO
3. EIFWALLR
4. EYEINHG
5. TUCALRIFMOT
6. OTEPHYON
7. TPDINNNLACEI
8. KERFMRWOA

Bonusopdracht: Snel denken

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

1	Banen in cyberbeveiliging			
2	Redenen om software bij te werken			
3	Dingen die een firewall kan blokkeren			
4	Waarschuwingssignalen in een e-mail			
5	Dingen waarvan je een back-up maakt			
6	Bekende soorten cyberaanvallen			
7	Dingen die een honeypot kan lokken			
8	Informatie die je nooit zou moeten delen			
9	Tekenen dat een computer is geïnfecteerd			
10	Films of series over hackers			
11	Beveiligingslagen die je kunt opbouwen			
12	Dingen om te oefenen tijdens een beveiligingsoefening			
13	Beveiligingstools die je kent			
14	Mensen die je om IT-hulp kunt vragen			
15	Woorden die met 'cyber' beginnen			

Controlepunt 8: Casestudy's cyberbeveiliging

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

CASESTUDY 1: HERSTELSTRATEGIE NA RANSOMWARE



Scenario: Een bedrijfsnetwerk is geïnfecteerd met ransomware, waardoor kritieke databases zijn vergrendeld. De aanvallers eisen een uitbetaling van $100.000 in cryptovaluta. Het bedrijf heeft offline back-ups van 24 uur geleden.

Discussievraag: analyseer de risico's van betalen en beoordeel de herstelstrategie.

CASESTUDY 2: VERDEDIGING TEGEN CREDENTIAL STUFFING



Scenario: Een online dienst wordt getroffen door een credential-stuffingaanval, waarbij hackers miljoenen combinaties van gebruikersnaam en wachtwoord uitproberen die van andere sites zijn gestolen.

Discussievraag: Beschrijf in detail het mechanisme van deze aanval en schets twee verdedigingssystemen.

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

2	5	22	5	9	12	9	7		19	25	19	20	5	13	5	14	13	5	20
								13	21	12	20	9	6	1	3	20	15	18	
							1	21	20	8	5	14	20	9	3	1	20	9	5

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 het hoofddoel van cyberbeveiliging?

Het hoofddoel is het beschermen van netwerken, apparaten en gegevens tegen ongeautoriseerde toegang, aanvallen en onbedoelde schade.

Q2: Waarin verschilt phishing van spearphishing?

Phishing is een brede e-mailcampagne gericht op willekeurige gebruikers, terwijl spearphishing zich richt op specifieke personen met behulp van persoonlijke gegevens.

Q3: Wat is een netwerkfirewall?

Een firewall is een netwerkbeveiligingssysteem dat inkomend en uitgaand verkeer bewaakt en filtert op basis van vooraf gedefinieerde beveiligingsregels.

Q4: Waarom is multifactorauthenticatie (MFA) noodzakelijk?

MFA voegt een cruciale verdedigingslaag toe en voorkomt toegang, zelfs als aanvallers de primaire wachtwoordgegevens stelen of kraken.

Q5: Wat definieert een computervirus?

Een virus is zichzelf vermenigvuldigende malware die zich aan schone bestanden hecht en zich na uitvoering over systemen verspreidt.

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

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

Q6: Hoe vergrendelt ransomware lokale data?

Ransomware gebruikt cryptografische algoritmen om gebruikersbestanden te versleutelen, waardoor ze onleesbaar worden totdat een ontsleutelingssleutel wordt toegepast.

Q7: Wat is een zero-day-kwetsbaarheid?

Een zero-day is een beveiligingslek in software dat de leverancier niet kent, waardoor er geen tijd is om een patch te ontwikkelen voordat het wordt misbruikt.

Q8: Welke rol speelt het NIST-raamwerk?

Het NIST-raamwerk biedt vrijwillige richtlijnen en standaarden om organisaties te helpen cyberbeveiligingsrisico's te beheersen en te verkleinen.

Q9: Wat is een plan voor het afhandelen van beveiligingsincidenten?

Het is een gedocumenteerde reeks procedures voor het opsporen, indammen en herstellen van beveiligingsincidenten en netwerkcompromittering.

Q10: Hoe maakt social engineering misbruik van gebruikers?

Social engineering gebruikt psychologische manipulatie om medewerkers ertoe te verleiden wachtwoorden prijs te geven of schadelijke bestanden te downloaden.

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

Verken geavanceerde technische aspecten van beveiligingsframeworks, malwareanalyse en gegevenscompliance.

Q1: Hoe overweldigt een DDoS-aanval webservers?

Een DDoS-aanval coördineert miljoenen gekaapte botnetapparaten om een server te overspoelen met verkeer, waardoor de bandbreedte en CPU-limieten uitgeput raken.

Q2: Wat is het verschil tussen symmetrische en asymmetrische versleuteling?

Symmetrische versleuteling gebruikt één sleutel voor versleutelen en ontsleutelen, terwijl asymmetrische versleuteling een publiek en privé sleutelpaar gebruikt.

Q3: Hoe voeren hackers SQL-injectieaanvallen uit?

Aanvallers voeren schadelijke SQL-opdrachten in via formuliervelden, waardoor de backenddatabase onbevoegd gebruikersgegevens vrijgeeft.

Q4: Wat is laterale beweging bij netwerkinbraken?

Het is de techniek waarbij aanvallers de eerste toegang tot een server misbruiken om andere onderling verbonden systemen in het interne netwerk te compromitteren.

Q5: Hoe leidt DNS-spoofing webverkeer om?

DNS-spoofing wijzigt de cacherecords van nameservers, waardoor legitieme gebruikers naar kwaadaardige lookalike-websites worden geleid in plaats van naar de beoogde domeinen.

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

Verken geavanceerde technische aspecten van beveiligingsframeworks, malwareanalyse en gegevenscompliance.

Q6: Wat is een hardwarematige beveiligingstoken?

Het is een fysiek apparaat (zoals een YubiKey) dat cryptografische authenticatiebewijzen genereert en maximale verdediging biedt tegen phishing op afstand.

Q7: Hoe gebruiken beveiligingsteams lokaas-honeypots?

Teams zetten decoyservers buiten de productieomgeving in om inbraken vroeg te detecteren en de aanvalspatronen van onbevoegden te analyseren.

Q8: Wat is het principe van least privilege?

Het is de beveiligingsstandaard om toegangsrechten van gebruikers te beperken tot het absolute minimum dat nodig is om hun functie uit te voeren.

Q9: Hoe misbruikt een man-in-the-middle-aanval verbindingen?

Een aanvaller onderschept en wijzigt de communicatie tussen twee apparaten op onversleutelde netwerken en steelt sessietokens en inloggegevens.

Q10: Wat zijn indicators of compromise (IOC's)?

IOC's zijn forensische aanwijzingen, zoals ongebruikelijke wijzigingen in het register of verdacht IP-verkeer, die laten zien dat een systeem is binnengedrongen.

Deel 11: 10 cyberbeveiligingsfeiten en inzichten uit de praktijk

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

1. BEVEILIGINGSINZICHT

Aanvallers scannen voortdurend het internet op kwetsbare servers en sturen phishingmails naar de inboxen van medewerkers.

2. BEVEILIGINGSINZICHT

Menselijke fouten, zoals het klikken op phishinglinks, spelen vaak een rol bij datalekken, en daarom is training belangrijk.

3. BEVEILIGINGSINZICHT

De kosten van een datalek omvatten juridische boetes, klantverloop, onderzoek en herstel, en kunnen oplopen tot miljoenen dollars.

4. BEVEILIGINGSINZICHT

Phishingbestendige MFA, zoals hardwarematige beveiligingssleutels, is het sterkste type MFA en de standaard die CISA aanbeveelt. [2]

5. BEVEILIGINGSINZICHT

Ransomware blijft een grote dreiging voor bedrijfsnetwerken, en CISA dringt aan op offline, versleutelde back-ups als belangrijke verdediging. [4]

6. BEVEILIGINGSINZICHT

Het NIST Cybersecurity Framework 2.0 (2024) kent zes kernfuncties: Govern (besturen), Identify (identificeren), Protect (beschermen), Detect (detecteren), Respond (reageren) en Recover (herstellen). [1]

7. BEVEILIGINGSINZICHT

Credential-stuffingbots testen op grote schaal gelekte combinaties van gebruikersnaam en wachtwoord op inlogportalen van banken en webwinkels.

8. BEVEILIGINGSINZICHT

Wereldwijd bestaan er markten voor zero-day-exploits, waar ernstige kwetsbaarheden voor grote bedragen kunnen worden verkocht voordat ze zijn gepatcht.

9. BEVEILIGINGSINZICHT

Een honeypot-lokaas meldt inbraakwaarschuwingen onmiddellijk, omdat legitieme gebruikers geen reden hebben om er toegang toe te krijgen.

10. BEVEILIGINGSINZICHT

Transport Layer Security (TLS) versleutelt browsersessies en voorkomt het afluisteren van pakketten op openbare wifi-netwerken.

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] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[2] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[3] 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

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

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

[6] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.
https://csrc.nist.gov/pubs/sp/800/61/r3/final

[7] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[8] OWASP. (n.d.). SQL Injection.
https://owasp.org/www-community/attacks/SQL_Injection

Antwoordsleutel: Controlepunt 1 - Meerkeuze

1 **Phishingaanvallen** PHISHING — **Juist antwoord: A**

DOCENTENNOTITIE

Phishingcampagnes proberen met nagemaakte e-mails inloggegevens en gevoelige gebruikersgegevens te stelen. Bron: OWASP Secure Configuration.

2 **Accountbescherming** MFA-SLEUTEL — **Juist antwoord: A**

DOCENTENNOTITIE

Multifactorauthenticatie (MFA) met hardwaretokens biedt de sterkste verdediging voor accounttoegang. Bron: NIST Digital Identity.

3 **Ransomwaredreiging** RANSOMWARE — **Juist antwoord: A**

DOCENTENNOTITIE

Ransomware versleutelt kritieke systemen en gegevens en eist betaling in cryptovaluta voor ontsleutelingssleutels. Bron: Center for Internet Security (CIS).

4 **Zero-daykwetsbaarheid** ZERO-DAY — **Juist antwoord: A**

DOCENTENNOTITIE

Zero-day-bedreigingen maken misbruik van ongepatchte, onbekende beveiligingslekken voordat een patch van de leverancier beschikbaar is. Bron: OWASP Secure Configuration.

5 **Beveiligingsframeworks** FRAMEWORKS — **Juist antwoord: A**

DOCENTENNOTITIE

Raamwerken zoals NIST bieden gestructureerde richtlijnen om organisaties te helpen cyberrisico's te beheren en te verkleinen. Bron: NIST Digital Identity.

Antwoordsleutel: Controlepunt 2 - Waar of onwaar

6 **Gerichte phishing** PHISHING — **Juist antwoord: Onwaar**

DOCENTENNOTITIE

Phishingaanvallen richten zich zowel op bedrijfsnetwerken als op persoonlijke accounts om de aanvalsmogelijkheden uit te breiden. Bron: OWASP Secure Configuration.

7 **Vraag 7** — **Juist antwoord: Waar**

DOCENTENNOTITIE

MFA vereist een tweede factor, dus een gestolen wachtwoord alleen is meestal niet genoeg om in te loggen.

8 **Verkeersfirewall** FIREWALL — **Juist antwoord: Waar**

DOCENTENNOTITIE

Firewalls controleren verkeer op specifieke netwerkpoorten en blokkeren het om ongeautoriseerde verbindingen te filteren. Bron: Center for Internet Security (CIS).

9 **Reactie op zero-days** ZERO-DAY — **Juist antwoord: Onwaar**

DOCENTENNOTITIE

Het verhelpen van zero-day-fouten vereist codepatches en WAF-filtering, omdat er nog geen signaturen bestaan. Bron: OWASP Secure Configuration.

10 **Lokaas-honeypots** HONEYPOT — **Juist antwoord: Waar**

DOCENTENNOTITIE

Honeypots zijn misleidende servers die beveiligingsteams gebruiken om kwaadwillenden te lokken, te waarschuwen en te bestuderen. Bron: Center for Internet Security (CIS).

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

D 1. Ransomwaredreiging	G 2. Multifactorauthenticatie	E 3. Zero-day-exploit	H 4. Lokaas-honeypot
C 5. Inbraakfirewall	B 6. Incidentrespons	F 7. Wachtwoordhygiëne	A 8. Beveiligingsraamwerk

CONTROLEPUNT 3: ANTWOORDEN KERNBEGRIPPEN

1 FIREWALL	2 EXPLOIT	3 PHISHING	4 MALWARE
5 HYGIËNE	6 VERSLEUTELING		

CONTROLEPUNT 6, ALTERNATIEF: ANTWOORDEN WOORDEN KOPPELEN

1 E – FIREWALL	2 F – INCIDENTPLAN	3 A – RANSOMWARE	4 B – MULTIFACTOR
5 G – HYGIENE	6 H – FRAMEWORK	7 C – ZERODAYEXPLOIT	8 D – HONEYPOT

DISCUSSIENOTITIES VOOR DOCENTEN

Kernbegrippen:
Controleer of leerlingen Ransomwaredreiging, Multifactorauthenticatie en Zero-day-exploit 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.

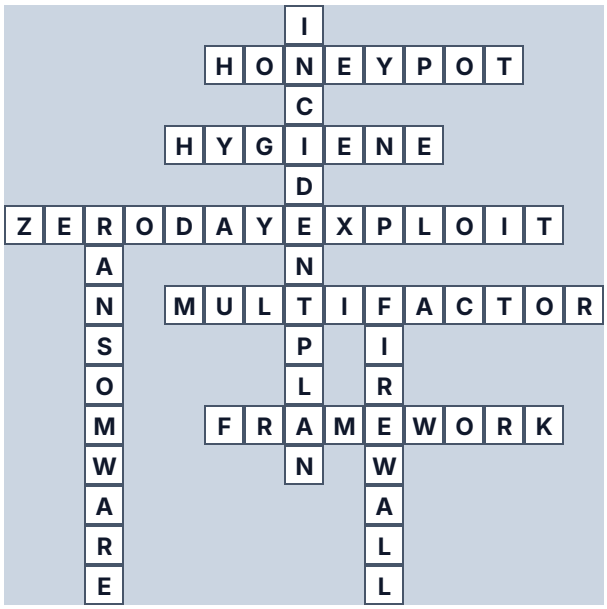
Bronnen beoordelen:
Laat leerlingen ten minste één bewering controleren aan de hand van de bronnen in het werkblad en bespreek waarom cijfers, prijzen en regels kunnen veranderen.

Puzzelsleutels en docentennotities

OPLOSSING WOORDZOEKER

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

OPLOSSING VAN DE KRUISWOORDPUZZEL



DOCENTENGIDS VOOR DE OPLOSSINGEN VAN DE KRUISWOORDPUZZEL

HORIZONTAAL

2 horizontaal: HONEYPOT Lokvogelsysteem dat is opgezet om kwaadwillenden te lokken en te analyseren (8 letters)

3 horizontaal: HYGIENE Best practices voor het beheren van inloggegevens en authenticatiesleutels (7 letters)

4 horizontaal: ZERODAYEXPLOIT Misbruik van een kwetsbaarheid voordat de leverancier een patch uitbrengt (14 letters)

6 horizontaal: MULTIFACTOR Beveiligingsverificatie waarvoor twee of meer authenticatiefactoren nodig zijn (11 letters)

8 horizontaal: FRAMEWORK Gestructureerde richtlijnen zoals NIST waarmee cyberrisico's worden beheerd (9 letters)

VERTICAAL

1 verticaal: INCIDENTPLAN Gestructureerd plan voor het afhandelen en beperken van beveiligingsincidenten (12 letters)

5 verticaal: RANSOMWARE Malware die gegevens versleutelt en financiële betaling eist voor ontsleuteling (10 letters)

7 verticaal: FIREWALL Netwerkbarrière die verkeer filtert op basis van beveiligingsregels (8 letters)

Sleutel voor husselwoorden en coderaadsel

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

SLEUTEL WOORDEN ORDENEN

1. RWMOARAESN — **RANSOMWARE**
2. DEARYIZOETPLXO — **ZERODAYEXPLOIT**
3. EIFWALLR — **FIREWALL**
4. EYEINHG — **HYGIENE**
5. TUCALRIFMOT — **MULTIFACTOR**
6. OTEPHYON — **HONEYPOT**
7. TPDINNNLACEI — **INCIDENTPLAN**
8. KERFMRWOA — **FRAMEWORK**

SLEUTEL VOOR DE GEHEIME CODE-OPDRACHT

"BEVEILIG SYSTEMEN MET MULTIFACTOR AUTHENTICATIE"

Antwoordsleutel casestudy's

A Casestudy 1: Herstelstrategie na ransomware

Oplossing voor docenten

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Scenarioanalyse: Een bedrijfsnetwerk is geïnfecteerd met ransomware, waardoor kritieke databases zijn vergrendeld. De aanvallers eisen een uitbetaling van $100.000 in cryptovaluta. Het bedrijf heeft offline back-ups van 24 uur geleden.
- Aanbevolen strategie en oplossing: Risico's van betalen: Betalen garandeert niet dat bestanden worden ontsleuteld, bestempelt het bedrijf als een betalend doelwit en financiert criminele activiteiten. Herstelstrategie: Het team moet geïnfecteerde hosts isoleren, gecompromitteerde servers wissen en gegevens herstellen vanaf offline back-ups. Het moet de oorspronkelijke toegangsvector (phishing of exploit) dichten om directe herinfectie te voorkomen.

B Casestudy 2: Verdediging tegen credential stuffing

Oplossing voor docenten

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Scenarioanalyse: Een online dienst wordt getroffen door een credential-stuffingaanval, waarbij hackers miljoenen gebruikersnaam-wachtwoordcombinaties testen die van andere sites zijn gestolen.
- Aanbevolen strategie en oplossing: Mechanisme: Aanvallers maken misbruik van hergebruik van wachtwoorden op verschillende sites en loggen met geautomatiseerde bots in op gebruikersaccounts. Verdediging: 1. Meervoudige verificatie (MFA) blokkeert inlogpogingen, zelfs als het wachtwoord klopt. 2. Het toepassen van snelheidsbeperking (rate limiting) en CAPTCHA's blokkeert geautomatiseerd botverkeer dat de inlogeindpunten bestookt.