Bijlage 2: Communicatie beveiligingsincidenten

Veel beveiligingsincidenten zijn in te delen in één van onderstaande vijf categorieën.

Openbaarmaking van niet-openbare informatie
Het expres of onbedoeld openbaar maken (lekken) of wissen van niet-openbare informatie, met inbegrip van privacygevoelige informatie.

Vermissing of diefstal van bedrijfsmiddelen
Diefstal of het kwijt raken van apparaten die door de gemeente worden beheerd. Denk hierbij aan een mobiele telefoon, tablet, laptop, toegangspasje of token.

Besmetting met schadelijke software (malware/virus)
Een besmetting van een werkstation of ander bedrijfsmiddel met schadelijke software, ook wel: malware. Hieronder worden ook virussen en cryptoware verstaan.

Aanval op de digitale infrastructuur
Een doelgerichte aanval op onze websites, (web)applicaties of servers met het doel niet-openbare informatie te verkrijgen of de digitale infrastructuur te ontregelen.

Storing in hardware door stroomuitval, brand of water
Een brand of wateroverlast (lekkage) in ruimten waar zich vitale ICT voorzieningen bevinden die leidt tot een verstoring van onze dienstverlening.

Op de volgende pagina’s staat de communicatiestrategie voor elk van bovenstaande vijf beveiligingsincidenten beknopt weergegeven.

Beveiligingsincident - Openbaarmaking van niet-openbare informatie

Korte omschrijving
Het expres of onbedoeld openbaar maken (lekken) of wissen van niet-openbare informatie, met inbegrip van privacygevoelige informatie.

Primaire doel van communicatie
- Vertrouwen behouden of herstellen bij onze stakeholders.
- Handelingsperspectief bieden aan stakeholders / betrokkenen bijvoorbeeld om (verdere) schade te voorkomen of te beperken.
- Bewustwording en alertheid op het gebied van gegevensbescherming bij medewerkers en bestuurders vergroten.

Stakeholders
- Betrokkenen: de persoon of personen van wie persoonsgegevens openbaar is/zijn gemaakt
- Portefeuillehouder: burgemeester en/of wethouder met Bedrijfsvoering in portefeuille
- Gemeentesecretaris
- Persoon die het beveiligingsincident heeft gemeld
- Inwoners van de gemeente Heemskerk
- Lokale / landelijke media (afhankelijk van de ernst van het datalek)
- Ketenpartners (afhankelijk van de aard van het datalek)
- Autoriteit Persoonsgegevens (AP)
- Informatie Beveiligings Dienst (IBD)

Deze lijst wordt op basis van het concrete incident door het CSIRT samen met de communicatieadviseur waar nodig bijgesteld / aangevuld.

Communicatietaken op hoofdlijnen

Wie	**Taak**	**Hulpmiddelen***
Portefeuillehouder (pfho)	Woordvoering, betekenisgeving en handelingsperspectief ▪ richting college en raad ▪ extern *Bij incidenten met grote impact*	▪ Kernboodschap ▪ Afstemmingsoverleg pfho, CISO, gemeentesecretaris, communicatieadviseur
Gemeentesecretaris	Woordvoering, betekenisgeving en handelingsperspectief intern *Bij incidenten met grote impact*	▪ Kernboodschap ▪ Afstemmingsoverleg
CISO	▪ Woordvoering *in overige gevallen* ▪ Betrekken pfho ▪ Betrekken ketenpartners ▪ Informeren melder incident ▪ Melden bij IBD	▪ Kernboodschap ▪ Afstemmingsoverleg ▪ Overleg CSIRT ▪ Overleg met ketenpartners (frequentie bepalen) ▪ Rapportages (sociale) media

FG	▪ Informeren betrokkenen ▪ Melden bij AP	▪ Kernboodschap ▪ Afstemmingsoverleg ▪ Overleg CSIRT ▪ Overleg met ketenpartners (frequentie bepalen) ▪ Rapportages (sociale) media
Communicatieadviseur	▪ Advisering pfho, secretaris, CISO ▪ Coördinatie interne en externe communicatie ▪ Productie communicatiemiddelen	▪ Afstemmingsoverleg ▪ Afstemmingsoverleg communicatie ▪ Q&A, berichtgeving op intranet, brief, persbericht, persgesprek enz
KCC	Informeren inwoners *bij incidenten met grote impact*	Q&A
Webredactie	▪ Informeren inwoners ▪ Monitoring en rapportage (sociale) media *bij incidenten met grote impact*	▪ Q&A, ▪ nieuwsberichten via website ▪ sociale media
Ketenpartners	Informeren achterban	▪ Overleg met CISO en adviseur communicatie ▪ Kernboodschap ▪ Q&A

* Overzicht communicatiemiddelen en medialijst beschikbaar bij team communicatie. .

Kernboodschap

De kernboodschap gaat in op deze aspecten en geeft een antwoord op deze vragen:

- Hoe heeft het lekken van deze informatie plaats kunnen vinden? Of, als dat nog niet bekend is: Wat doen we om de oorzaak van het lek te achterhalen?
- Hoeveel informatie is er gelekt en wat was de exacte aard van de informatie? Of, als dat nog niet bekend is: wat doet de gemeente om te achterhalen hoeveel informatie er is gelekt en wat de exacte aard van de informatie is?
- Wat zijn de consequenties voor medewerkers, inwoners, bedrijven, ketenpartners enz. van de gemeente?
- Welke acties kunnen of moeten zij eventueel nemen om schade te beperken of te voorkomen?
- Welke maatregelen heeft de gemeente genomen of neemt de gemeente om het ‘lek’ te dichten en in de toekomst te voorkomen dat het weer gebeurt?

Beveiligingsincident - Vermissing of diefstal van bedrijfsmiddelen

Korte omschrijving
Diefstal of het kwijt raken van apparaten die door de gemeente worden beheerd. Denk hierbij aan een mobiele telefoon, tablet, laptop, toegangspasje of token.

Is niet vast te stellen wat de oorzaak van het incident is, welke informatie er op het apparaat staat, of c.q. hoe de informatie te ontsluiten is? Dan wordt het automatisch (ook) beveiligingsincident 'Openbaarmaking van niet-openbare informatie'.

Primaire doel van communicatie
- Vertrouwen behouden of herstellen bij onze stakeholders.
- Handelingsperspectief bieden aan stakeholders / betrokkenen bijvoorbeeld om (verdere) schade te voorkomen of te beperken.
- Bewustwording en alertheid op het gebied van gegevensbescherming bij medewerkers en bestuurders vergroten.

Stakeholders
- Portefeuillehouder: afhankelijk van de ernst van het datalek
- Eigenaar of gebruiker van het apparaat en zijn leidinggevende
- Facilitaire Dienst (FD); apparaat in beheer & toegangspasjes en token
- Politie voor het doen van aangifte in het geval van diefstal
- Verzekeraar indien van toepassing
- Lokale / landelijke media (afhankelijk van de ernst van het datalek)
- Inwoners gemeente Heemskerk (afhankelijk van de ernst van het datalek)

Deze lijst wordt op basis van het concrete incident door het CSIRT samen met de communicatieadviseur waar nodig bijgesteld / aangevuld.

Communicatietaken op hoofdlijnen

Wie	Taak	Hulpmiddelen*
Portefeuillehouder (pfho)	Woordvoering, betekenisgeving en handelingsperspectief ▪ richting college en raad ▪ extern *Bij incidenten met grote impact*	▪ Kernboodschap ▪ Afstemmingsoverleg pfho, CISO, gemeentesecretaris, adviseur communicatie
Gemeentesecretaris	Woordvoering, betekenisgeving en handelingsperspectief intern *Bij incidenten met grote impact*	▪ Kernboodschap ▪ Afstemmingsoverleg

CISO	▪ Woordvoering *in overige gevallen* ▪ Betrekken pfho ▪ Informeren eigenaar/gebruiker apparaat ▪ Betrekken FD ▪ Inlichten verzekering ▪ Aangifte bij politie	▪ Kernboodschap ▪ Afstemmingsoverleg ▪ Overleg CSIRT ▪ Rapportages (sociale) media
Communicatieadviseur	▪ Advisering pfho, secretaris, CISO ▪ Coördinatie interne en externe communicatie ▪ Productie communicatiemiddelen	▪ Afstemmingsoverleg ▪ Afstemmingsoverleg communicatie ▪ Q&A, berichtgeving op intranet, persbericht, persgesprek, brief, enz.
KCC	Informeren inwoners *Bij incidenten met grote impact*	Q&A
Webredactie	▪ Informeren inwoners ▪ Monitoring en rapportage (sociale) media *Bij incidenten met grote impact*	▪ Q&A, ▪ nieuwsberichten via website ▪ sociale media

* Overzicht communicatiemiddelen en medialijst beschikbaar bij team communicatie.

Kernboodschap

De kernboodschap gaat in op deze aspecten en geeft een antwoord op deze vragen:

- Hoe heeft de diefstal plaats kunnen vinden? Of, als dat nog niet bekend is: wat doet de gemeente om de oorzaak te achterhalen?
- Hoeveel informatie is er gelekt en wat was de exacte aard van de informatie? Of, als dat nog niet bekend is: wat doet de gemeente om te achterhalen hoeveel informatie er is gelekt en wat de exacte aard van de informatie is?
- Stond er gevoelige informatie (persoonsgegevens) op het apparaat?
- Is toegang tot het apparaat mogelijk?
  Bijv. alleen na ontgrendeling met bijvoorbeeld een wachtwoord of pincode.
- Staat er informatie (lokaal) opgeslagen op het apparaat? Zo ja, is deze informatie versleuteld of niet?
- Is het apparaat op afstand te lokaliseren dan wel wissen door Automatisering?
  Door het gebruik van een zgn. Mobile Device Management (MDM) oplossing.
- Wat zijn de consequenties voor medewerkers, inwoners, bedrijven, ketenpartners enz. van de gemeente?
- Welke acties kunnen of moeten zij eventueel nemen om schade te beperken of te voorkomen?
- Welke maatregelen heeft de gemeente genomen of neemt de gemeente om een dergelijke diefstal in de toekomst te voorkomen?

Beveiligingsincident - Besmetting met schadelijke software (malware/virus)

Korte omschrijving
Een besmetting van een werkstation of ander bedrijfsmiddel met schadelijke software, ook wel: malware. Hieronder worden ook virussen en cryptoware verstaan.

Primaire doel van communicatie
- Vertrouwen behouden of herstellen bij onze stakeholders.
- Handelingsperspectief bieden aan stakeholders / betrokkenen bijvoorbeeld om (verdere) schade te voorkomen of te beperken.
- Bewustwording en alertheid op het gebied van gegevensbescherming bij medewerkers en bestuurders vergroten.

Stakeholders
- Eigenaar/gebruiker van het apparaat waar de besmetting startte
- Automatisering (beheert netwerk en apparaten)
- Portefeuillehouder: burgemeester en/of wethouder met Bedrijfsvoering in portefeuille
- Gemeentesecretaris
- Medewerkers gemeente Heemskerk
- Lokale media (indien dienstverlening gemeente tijdelijk niet beschikbaar)
- Informatie Beveiligingsdienst (IBD)

Deze lijst wordt op basis van het concrete incident door het incident respons team samen met de communicatieadviseur waar nodig bijgesteld / aangevuld.

Communicatietaken op hoofdlijnen

Wie	Taak	Hulpmiddelen*
Portefeuillehouder (pfho)	Woordvoering, betekenisgeving en handelingsperspectief ▪ extern ▪ richting college en raad *Bij incidenten met grote impact*	▪ Kernboodschap ▪ Afstemmingsoverleg pfho, CISO, gemeentesecretaris, adviseur communicatie
Gemeentesecretaris	Woordvoering, betekenisgeving en handelingsperspectief intern *Bij incidenten met grote impact*	▪ Kernboodschap ▪ Afstemmingsoverleg
CISO	▪ Woordvoering *in overige gevallen* ▪ Betrekken pfho ▪ Betrekken Automatisering ▪ Informeren eigenaar apparaat ▪ Melden bij IBD ▪ Inlichten verzekering	▪ Kernboodschap ▪ Afstemmingsoverleg ▪ Overleg CSIRT ▪ Rapportages (sociale) media

	▪ Aangifte bij politie	
Communicatieadviseur	▪ Advisering pfho, secretaris, CISO ▪ Coördinatie interne en externe communicatie ▪ Productie communicatiemiddelen	▪ Afstemmingsoverleg ▪ Afstemmingsoverleg communicatie ▪ Q&A, berichtgeving op intranet, brief, persbericht, persgesprek, enz
KCC	Informeren inwoners *Bij incidenten met grote impact*	Q&A
Webredactie	▪ Informeren inwoners ▪ Monitoring en rapportage (sociale) media *Bij incidenten met grote impact*	▪ Q&A, ▪ nieuwsberichten via website ▪ sociale media

* Overzicht communicatiemiddelen en medialijst beschikbaar bij team communicatie.

Kernboodschap

De kernboodschap gaat in op deze aspecten en geeft een antwoord op deze vragen:

- Wat is de oorzaak van de besmetting? Of, als dat nog niet bekend is: wat doet de gemeente om de oorzaak te achterhalen?
  Denk aan het klikken op een phishing link, het openen van een malafide bijlage bij een e-mail, het installeren van onvertrouwde software of het inpluggen van een besmette USB-stick ***(geen namen noemen!)***.
- Om welk soort besmetting gaat het precies? Welk type malware?
- Hoe ver heeft de bestemming om zich heen kunnen grijpen? Zijn vitale delen van het netwerk ook blootgesteld aan de besmetting?
- Hoeveel tijd zat er tussen de besmetting en de signalering daarvan?
  Dit zegt iets over de mate van gegevensbescherming.
- Hoe snel is de besmetting ongedaan gemaakt door het terugzetten van een back-up?
- Hoeveel data zijn verloren gegaan?
- Wat zijn de consequenties voor medewerkers, inwoners, bedrijven, ketenpartners enz. van de gemeente?
- Welke acties kunnen of moeten zij eventueel nemen om schade te beperken of te voorkomen?
- Welke maatregelen heeft de gemeente genomen of neemt de gemeente om een besmetting als deze in de toekomst te voorkomen?
  Bijv. We blijven inzetten op bewustwording bij medewerkers en bestuurders om de alertheid op dit gebied te vergroten.

Beveiligingsincident - Aanval op de digitale infrastructuur

Korte omschrijving
Een doelgerichte aanval op onze websites, (web)applicaties of servers met het doel niet-openbare informatie te verkrijgen of de digitale infrastructuur te ontregelen.

Is bij de aanval ook niet-openbare informatie openbaar gemaakt? Dan wordt het automatisch beveiligingsincident 'Openbaarmaking van niet-openbare informatie'.

Primaire doel van communicatie
- Vertrouwen behouden of herstellen bij onze stakeholders.
- Handelingsperspectief bieden aan stakeholders / betrokkenen bijvoorbeeld om (verdere) schade te voorkomen of te beperken.
- Bewustwording en alertheid op het gebied van gegevensbescherming bij medewerkers en bestuurders vergroten.

Stakeholders
- Automatisering (die het netwerk en applicaties beheert)
- Portefeuillehouder: burgemeester en/of wethouder met Bedrijfsvoering in portefeuille
- Gemeentesecretaris
- Medewerkers gemeente Heemskerk
- Lokale media (indien dienstverlening gemeente tijdelijk niet beschikbaar)
- Informatie Beveiligingsdienst (IBD)

Deze lijst wordt op basis van het concrete incident door het incident respons team samen met de communicatieadviseur waar nodig bijgesteld / aangevuld.

Communicatietaken op hoofdlijnen

Wie	**Taak**	**Hulpmiddelen***
Portefeuillehouder (pfho)	Woordvoering, betekenisgeving en handelingsperspectief ▪ extern ▪ richting college en raad *Bij incidenten met grote impact*	▪ Kernboodschap ▪ Afstemmingsoverleg pfho, CISO, gemeentesecretaris, adviseur communicatie
Gemeentesecretaris	Woordvoering, betekenisgeving en handelingsperspectief intern *Bij incidenten met grote impact*	▪ Kernboodschap ▪ Afstemmingsoverleg
CISO	▪ Woordvoering *in overige gevallen* ▪ Betrekken pfho ▪ Betrekken Automatisering ▪ Melden bij IBD	▪ Kernboodschap ▪ Afstemmingsoverleg ▪ Overleg incident respons team ▪ Rapportages (sociale) media
Communicatieadviseur	▪ Advisering pfho, secretaris, CISO	▪ Afstemmingsoverleg

	▪ Coördinatie interne en externe communicatie ▪ Productie communicatiemiddelen	▪ Afstemmingsoverleg communicatie ▪ Q&A, berichtgeving op intranet, persbericht, persgesprek, brief, enz
KCC	Informeren inwoners *Bij incidenten met grote impact*	Q&A
Webredactie	▪ Informeren inwoners ▪ Monitoring en rapportage (sociale) media *Bij incidenten met grote impact*	▪ Q&A, ▪ nieuwsberichten via website ▪ sociale media

* Overzicht communicatiemiddelen en medialijst beschikbaar bij team communicatie.

Kernboodschap

De kernboodschap gaat in op deze aspecten en geeft een antwoord op deze vragen:

- Waarop was de aanval gericht? Wat was het doel?
- In hoeverre zijn de aanvallers geslaagd in het behalen van hun (vermoede) doel?
- Hoe en hoe snel had de gemeente in de gaten dat het om een doelgerichte aanval ging?
- Hoe (on)gebruikelijk is zo'n aanval?
  Dergelijke aanvallen zijn niet ongebruikelijk.
- Waarom is de gemeente gemeente Heemskerk aangevallen?
  Slachtoffers zijn in de meeste gevallen willekeurige doelwitten.
- Wat zijn de consequenties voor medewerkers, inwoners, bedrijven, ketenpartners enz. van de gemeente?
- Welke acties kunnen of moeten zij eventueel nemen om schade te beperken of te voorkomen?
- Welke tijdelijke en mogelijk permanente (immateriële) schade heeft de gemeente opgelopen als gevolg van de aanval?
- Welke maatregelen heeft de gemeente genomen of neemt de gemeente om een aanval als deze in de toekomst te voorkomen?
  Helemaal uitsluiten van een dergelijke aanval is nagenoeg onbetaalbaar. Op basis van de kosten en baten wordt een optimale graag van beveiliging bepaald (risico verlagen versus kosten van de maatregelen).

Beveiligingsincident - Storing in hardware door stroomuitval, brand of water

Korte omschrijving
Een brand of wateroverlast (lekkage) in ruimten waar zich vitale ICT voorzieningen bevinden die leidt tot een verstoring van onze dienstverlening.

Primaire doel van communicatie
- Vertrouwen behouden of herstellen bij onze stakeholders.
- Handelingsperspectief bieden aan stakeholders / betrokkenen bijvoorbeeld om (verdere) schade te voorkomen of te beperken.

Stakeholders
- Inwoners van de gemeente Heemskerk
- Medewerkers gemeente Heemskerk
- Gemeentesecretaris
- Burgemeester
- Automatisering (beheert de hardware en het netwerk)
- Lokale/landelijke media (afhankelijk van de ernst van de brand/wateroverlast)
- Ketenpartners
- Leveranciers
- Autoriteit Persoonsgegevens (AP)
- Informatie Beveiligingsdienst (IBD)
- Politie indien het vermoeden bestaat dat er sprake is van opzet

Deze lijst wordt op basis van het concrete incident door het incident respons team samen met de communicatieadviseur waar nodig bijgesteld / aangevuld.

Communicatietaken op hoofdlijnen

Wie	Taak	Hulpmiddelen*
Portefeuillehouder (pfho)	Woordvoering, betekenisgeving en handelingsperspectief ▪ extern ▪ richting college en raad *Bij incidenten met grote impact*	▪ Kernboodschap ▪ Afstemmingsoverleg pfho, CISO, gemeentesecretaris, adviseur communicatie
Gemeentesecretaris	Woordvoering, betekenisgeving en handelingsperspectief intern *Bij incidenten met grote impact*	▪ Kernboodschap ▪ Afstemmingsoverleg
CISO	▪ Woordvoering *in overige gevallen* ▪ Betrekken pfho ▪ Betrekken ketenpartners ▪ Informeren / betrekken leveranciers	▪ Kernboodschap ▪ Afstemmingsoverleg ▪ Overleg incident respons team ▪ Overleg ketenpartners

	▪ Melden bij IBD ▪ Aangifte bij politie	▪ Rapportages (sociale) media
FG	▪ Informeren betrokkenen ▪ Melden bij AP	▪ Kernboodschap ▪ Afstemmingsoverleg ▪ Overleg CSIRT ▪ Overleg met ketenpartners (frequentie bepalen) ▪ Rapportages (sociale) media
Communicatieadviseur	▪ Advisering pfho, secretaris, CISO ▪ Coördinatie interne en externe communicatie ▪ Productie communicatiemiddelen	▪ Afstemmingsoverleg ▪ Afstemmingsoverleg communicatie ▪ Q&A, berichtgeving op intranet, persbericht, persgesprek, brief, enz
KCC	Informeren inwoners *Bij incidenten met grote impact*	Q&A
Webredactie	▪ Informeren inwoners ▪ Monitoring en rapportage (sociale) media *Bij incidenten met grote impact*	▪ Q&A, ▪ nieuwsberichten via website ▪ sociale media
Ketenpartners	Informeren achterban	▪ Overleg met CISO en adviseur communicatie ▪ Kernboodschap ▪ Q&A

* Overzicht communicatiemiddelen en medialijst beschikbaar bij team communicatie.

Kernboodschap

De kernboodschap gaat in op deze aspecten en geeft een antwoord op deze vragen:

- Zijn er gewonden of doden gevallen bij de brand / wateroverlast?
- Wat is de oorzaak van de brand / wateroverlast? Of, als dat nog niet bekend is: wat doet de gemeente we om de oorzaak te achterhalen?
- Hoe heeft dit de vitale ICT-voorzieningen kunnen bereiken?
- Wat zijn de consequenties voor medewerkers, inwoners, bedrijven, ketenpartners enz. van de gemeente? Bijv. welk deel van de dienstverlening is wel en welk deel is niet beschikbaar als gevolg van het uitvallen van vitale ICT voorzieningen?
- Op welke termijn wordt de dienstverlening weer operationeel?
- Welke (materiële) schade heeft de gemeente opgelopen?
- Welke maatregelen heeft de gemeente genomen of neemt de gemeente om een situatie als deze in de toekomst te voorkomen?