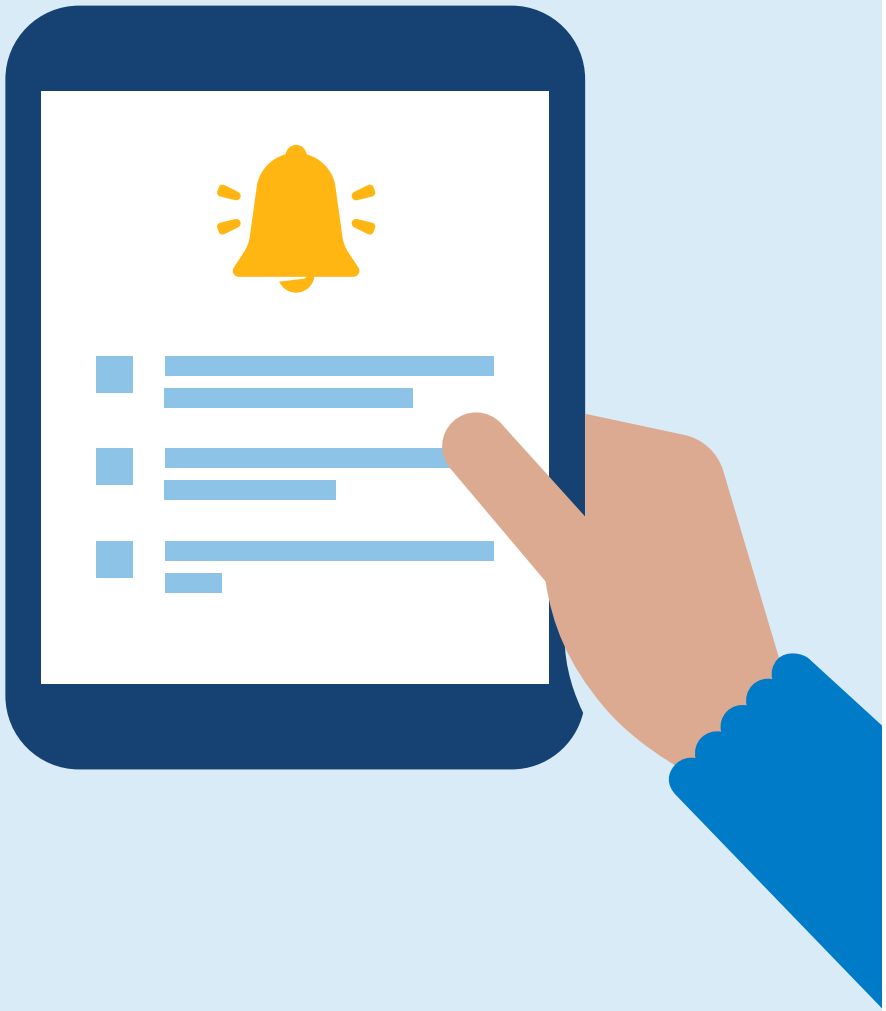
Ministerie van Economische Zaken



Cyber Incident Logboek

Leg het verloop van een incident vast.
Dit helpt bij het vinden van een oorzaak en bij het doen van aangifte of verzekeringsclaim.

Logboek beheerder

Naam _____

Te bereiken via _____

Logboek beheerder

Naam _____

Te bereiken via _____

digital trust center.

Incident details en categorie

Incident details

Naam van het incident _____

Datum van eerste melding __ __ __ __ __ __ __ __

Tijd van eerste melding ____ : ____

Korte beschrijving van het incident. Welke systemen, gegevens of processen zijn getroffen?

_____

Incident categorie

Selecteer de gepaste categorie van het incident

- ☐ Uitval van systemen
- ☐ Digitale inbraak
- ☐ Besmetting met virus of gijzelsoftware
- ☐ Datalek of datadiefstal
- ☐ Website onbereikbaar of gemanipuleerd
- ☐ Afpersing of fraude
- ☐ Anders, namelijk:

_____

Handige links

- Wat te doen bij een cyberincident
- Melden van een datalek

Incident tijdlijn

Een tijdlijn voor een cyberincident is een overzicht van alle gebeurtenissen die plaatsvinden vanaf het moment dat het cyberincident wordt ontdekt tot de volledige afhandeling daarvan.

Het doel van een tijdlijn is om inzicht te krijgen in de **oorzaak**, **effecten** en de **genomen maatregelen** tijdens het cyberincident.

Het bevat de **tijd en datum** van elke gebeurtenis, **welke systemen**, **gegevens en processen** zijn getroffen, de **maatregelen** die zijn genomen, **wie erbij betrokken was**, en **wanneer er met interne of externe partijen is gecommuniceerd**.

Indien van toepassing ook hoe en wanneer de bedrijfsvoering werd hersteld.

Gebeurtenis 1

Datum _____

Tijd ____ : ____

Door wie _____

Wat is er waargenomen?
Op welk systeem?
Bij welke gegevens of processen?

_____

Welke actie is ondernomen?

_____

Wat was het effect?

_____

Welke communicatie volgde?

_____

Melding en aanvullende opmerkingen

Melding

Zijn er persoonsgegevens bij het incident betrokken? ☐ Ja ☐ Nee

Zo ja, is er gemeld bij Autoriteit Persoonsgegevens? ☐ Ja ☐ Nee

Bij welke autoriteiten of wetshandhavingsinstanties is dit incident gemeld?

_____

Welke andere organisaties of ketenpartners zijn op de hoogte gesteld?

_____

Aanvullende opmerkingen

Aanvullende opmerkingen of commentaar

_____

Tip

Sla dit logboek op twee verschillende veilige locaties op zodat je logboek niet verloren gaat bij een zich ontwikkelend cyberincident.

Incident tijdlijn

Bij het opstellen van een tijdlijn is het belangrijk om te noteren **hoe het incident werd ontdekt**.

Voorbeelden hiervan zijn:

- De website of bedrijfsnetwerk is niet meer bereikbaar
- Bepaalde systemen zijn niet (goed) meer toegankelijk
- Vertrouwelijke informatie bevindt zich buiten de organisatie

Gebeurtenis 2

Datum _____

Tijd ____ : ____

Door wie _____

Wat is er waargenomen?
Op welk systeem?
Bij welke gegevens of processen?

_____

Welke actie is ondernomen?

_____

Wat was het effect?

_____

Welke communicatie volgde?

_____

Melding en aanvullende opmerkingen

Melding

Zijn er persoonsgegevens bij het incident betrokken? ☐ Ja ☐ Nee

Zo ja, is er gemeld bij Autoriteit Persoonsgegevens? ☐ Ja ☐ Nee

Bij welke autoriteiten of wetshandhavingsinstanties is dit incident gemeld?

_____

Welke andere organisaties of ketenpartners zijn op de hoogte gesteld?

_____

Aanvullende opmerkingen

Aanvullende opmerkingen of commentaar

_____

Tip

Sla dit logboek op twee verschillende veilige locaties op zodat je logboek niet verloren gaat bij een zich ontwikkelend cyberincident.

Incident tijdlijn

Gebeurtenis 3

Datum

Tijd

Door wie

Wat is er waargenomen?
Op welk systeem?
Bij welke gegevens of
processen?

Welke actie is ondernomen?

Wat was het effect?

Welke communicatie volgde?

Melding en aanvullende opmerkingen

Melding

Zijn er persoonsgegevens bij het incident betrokken? ☐ Ja ☐ Nee

Zo ja, is er gemeld bij Autoriteit Persoonsgegevens? ☐ Ja ☐ Nee

Bij welke autoriteiten of wetshandhavingsinstanties is dit incident gemeld?

_____

Welke andere organisaties of ketenpartners zijn op de hoogte gesteld?

_____

Aanvullende opmerkingen

Aanvullende opmerkingen of commentaar

_____

Tip

Sla dit logboek op twee verschillende veilige locaties op zodat je logboek niet verloren gaat bij een zich ontwikkelend cyberincident.

Incident tijdlijn

Gebeurtenis 4

Datum _____

Tijd ____ : ____

Door wie _____

Wat is er waargenomen?
Op welk systeem?
Bij welke gegevens of
processen?

_____

Welke actie is ondernomen?

_____

Wat was het effect?

_____

Welke communicatie volgde?

_____

Melding en aanvullende opmerkingen

Melding

Zijn er persoonsgegevens bij het incident betrokken? ☐ Ja ☐ Nee

Zo ja, is er gemeld bij Autoriteit Persoonsgegevens? ☐ Ja ☐ Nee

Bij welke autoriteiten of wetshandhavingsinstanties is dit incident gemeld?

_____

Welke andere organisaties of ketenpartners zijn op de hoogte gesteld?

_____

Aanvullende opmerkingen

Aanvullende opmerkingen of commentaar

_____

Tip

Sla dit logboek op twee verschillende veilige locaties op zodat je logboek niet verloren gaat bij een zich ontwikkelend cyberincident.

Handige links

- Wat te doen bij een cyberincident
- Melden van een datalek

digital trust
center.