white paper

TIPS VOOR CRISISCOMMUNICATIE BIJ CYBER.

COMPAIJEN
CRISISMANAGEMENT & COMMUNICATIE

INHOUDSOPGAVE

MEEST GETROFFENEN OP 1

- Bij cybercrisis kan je altijd denken aan de volgende doelgroepen: mensen van wie data mogelijk openbaar is geworden; mensen die eigenaar zijn van de data; mensen en organisaties die niet meer kunnen werken omdat hun kritieke processen verstoord zijn; een samenleving die mogelijk impact ervaart; leveranciers, medewerkers. Zorg dat je weet wie van hen allemaal getroffen en betrokken zijn en wie het meest getroffen zijn.

- De Autoriteit Persoonsgegevens (AP) heeft een webpagina met welke persoonsgegevens gevoelige data zijn.

AANSLUITEN BIJ DE BUITENWERELD

- Zorg eerst dat je een goed beeld hebt: Welke kennis over ICT en cyber hebben jouw klanten, leveranciers, medewerkers, inwoners of algemeen publiek? Wat vinden ze van de gebeurtenissen? En weten we wat ze moeten doen?

- Gebruik metaforen om uit te leggen wat er gebeurd is, maak het cyberverhaal weer visueel en begrijpelijk. “From ones and zero’s to villains and heroes”

- Wees empathisch: zorg dat je echt weet wat het voor mensen betekent dat dit gebeurd is. Ga luisteren en praten.

- De oorzaak is technisch, het gevolg niet

OPEN, EERLIJK EN TRANSPARANT ZIJN

- ‘Everything that can come out, will come out.’ Dus breng zelf ook de negatieve informatie naar buiten. Alleen zo kan je het vertrouwen houden.

- Niet bang zijn om met de billen bloot te gaan. Het is wat het is, maak de feiten niet mooier dan ze zijn. Dus niet ontkennen, liegen, bagatelliseren of anderen de schuld geven.

- Soms kan je iets niet vertellen, bijvoorbeeld omdat je de criminelen geen *credits* wilt geven of het niet in belang is van je klanten om volledige technische openheid te geven. Maar dat mag NOOIT iets zijn om je achter te verschuilen.

PRIORITEITEN STELLEN OP BASIS VAN VERANTWOORDELIJKHEID, URGENTIE EN IMPACT.

- Zorg dat je goed weet wie je crisispartners zijn, wie waarvoor verantwoordelijk is en wie het meest geraakt wordt door de uitval van ICT en bepaalde processen of het lekken van data.

- Ga als eerste die problemen oplossen waar jij verantwoordelijk voor bent en waarmee je de schade zo veel mogelijk beperkt voor de belangrijkste groepen. Communiceer ook primair hierover en met deze groepen.

- Vaak ligt bij cyber de focus op de eigen medewerkers. Zij ondervinden de meeste last van de ICT-verstoring en kunnen soms niet meer werken. Ook kunnen zij de schade verergeren of juist beperken. Maar onthoud: intern = extern.

- Zorg dat je op de hoogte bent van wie je security partners zijn en waar zij je bij kunnen helpen qua communicatie. Soms zijn er *incident responders* die het communicatieteam helpen de situatie te begrijpen en handvatten bieden voor een goede kernboodschap.

VERTEL STEEDS WAT JE WEET, NIET WEET EN WAT JE DOET.

1. Bij merkbare effecten in de buitenwereld: breng zo snel mogelijk een eerste bericht uit dat bestaat uit de volgende drie elementen:
    - *Wat is er gebeurd*: een feitelijk omschrijving van dat wat waarneembaar is. Eventueel termen cyber-incident of ICT-verstoring. Zonder afstemming met het crisisteam, management, en/of ICT)gebruik je NIET woorden als ‘hack’, ‘lek’, ‘ransomware-aanval’.
    - *Wat doen wij*: crisisteam bij elkaar, we onderzoeken wat er gebeurd is
    - *Waar en wanneer meer informatie*: volg onze website of social media voor meer informatie
2. Na overleg crisisteam zo snel mogelijk duidelijker en specifieker worden over wat er precies gebeurd is en welke woorden je daarvoor gebruikt: hack, datalek, etc.
3. Daarna steeds in een vast ritme (elk uur; elke dag) updates blijven geven
4. Gebruik daarbij weer de constructie:
    - *We know*: dit weten we wel; dit weten we niet
    - *We care*: duiding, wat betekent dit voor getroffenen, empathie, emotie
    - *We do*: wat doen wij, wat moet je doen (en laten)
    - *We’ll be back*: waar vind je meer informatie
5. Geef procesinformatie zoals:
    - We hebben aangifte gedaan bij politie.
    - We hebben een extern gespecialiseerde partij in de hand genomen om het incident zo snel mogelijk te verhelpen.
    - We hebben melding gemaakt bij de AP van een datalek.

BONUS

BOUW EEN BUFFER VAN VERTROUWEN

- *Communiceer ook vóór de crisis*
- Wacht niet tot een cyberincident met communiceren over cybersecurity. Begin op tijd, ook als er niets aan de hand is. Wel op een manier die past bij het moment, het kanaal en je doelgroep.
- Laat bijvoorbeeld in een nieuwsbrief of op je website zien hoe je data beschermt, hoe je bent voorbereid op een cybercrisis en met welke dilemma's je te maken hebt. Daarmee laat je zien dat je het onderwerp serieus neemt.
- Misschien leest niet iedereen die berichten meteen. Toch bouw je hiermee iets op: een buffer van vertrouwen. Organisaties staan qua vertrouwen standaard op nul. Een crisis kan je dan snel op -1 of -2 zetten. Maar als je al zichtbaar werk maakt van cybersecurity, begin je op +2 of +3. Je kunt de klap dan beter opvangen en blijft bij een crisis boven de nul-lijn.
- Communicatie over cybersecurity mag geen window dressing zijn. Het is een kans om te laten zien dat je de boel écht op orde hebt — en dat je werkt aan verbetering.