Is de politie zelf getroffen door de cyberaanval?
De politie is niet getroffen door de cyberaanval, maar heeft sinds gistermiddag 27 juni voorzorgsmaatregelen genomen. Hierdoor zijn functionaliteiten op onze website politie.nl tijdelijk niet of niet volledig beschikbaar.

Doet de politie onderzoek naar deze cyberaanval?
De politie doet onderzoek samen met alle voor ons relevante internationale opsporingspartners en diverse private cyber securitybedrijven.

Waar richt het onderzoek van de politie zich op?
Het onderzoek richt zich op het opsporen van daders, het stoppen of verstoren van de cyberaanval, en het beperken van schade bijvoorbeeld door preventie-adviezen te geven.

Is er al zicht op wie er achter deze cyberaanval zit?
Aangezien het gaat om een wereldwijde cyberaanval, werkt de politie nauw samen met internationale opsporingspartners. Het onderzoek is in volle gang.

Hoe veel Nederlandse slachtoffers hebben zich gemeld bij de politie?
Het is bekend dat enkele grote internationale bedrijven, gevestigd in Nederland, getroffen zijn door de cyberaanval.

Komen tegengehouden e-mails (afkomstig van buiten de organisatie) op een later moment na de storing wel binnen?
De mails die van buiten verzonden zijn, staan in de wachtrij bij de provider waar vanaf de mail is verzonden. Op het moment dat de emailvoorziening van de politie hersteld is, zullen deze e-mails in principe allemaal alsnog afgeleverd worden. We zeggen 'in principe', omdat het aan de provider van de afzender is om dit te doen. In de meeste gevallen gebeurt dit automatisch, maar in theorie is het mogelijk dat providers opgeslagen e-mails voor een te korte tijd opslaan. Deze kans achten wij niet groot.

Als deze e-mails later alsnog binnenkomen, mogen deze dan wel geopend worden? (incl. bijlages en links)
In principe mogen deze mails dan gewoon geopend worden. Ook de bijbehorende bijlages en links. Het kan natuurlijk wel zo zijn dat, ondanks alle getroffen maatregelen, er toch een mail tussendoor glipt die wel een virus bevat. We vragen iedereen dan ook om extra alert te zijn.

Mogen bijlages uit oude mails van buiten de organisatie (ontvangen voor 27 juni, ca. 10.00u) wel geopend worden?
Ja, deze mails mogen gewoon geopend worden. Maar ook hier vragen we aan jullie om extra alert te zijn. Vertrouw je een mail of afzender niet? Twijfel je? Open de mail dan niet.

Hoe weet je of een email (of bijlage/link) betrouwbaar is/geopend kan worden?
Het is moeilijk om hier een zwart/wit antwoord op te geven. De mensen die achter cyberaanvallen zitten, weten steeds beter een mooier een virus en/of nep mail te verpakken. Er zijn wel een aantal controlevragen die je jezelf kunt stellen, namelijk:

- Verwacht je een e-mail van dit persoon?
- Ken je de persoon die jou een e-mail stuurt?
- En zo ja: is het legitiem dat hij/zij je mailt?
- Is er sprake van een afwijkend e-mailadres of onderwerp regel?

Twijfel je over een e-mail of afzender? Open de mail dan niet. Of neem, indien mogelijk, telefonisch contact op met dit persoon en vraag naar de inhoud/reden van de e-mail.

Krijgen afzenders van externe partijen een melding dat hun e-mail op dit moment niet aankomt?
Dat gebeurt niet standaard. Het ligt aan de provider van de afzender of hij/zij geïnformeerd wordt. In het geval dat zij geïnformeerd worden, zal dat zijn met een mail met de mededeling dat de mail niet afleverbaar is.

Is klikken op een mail al gevaarlijk? Of wordt het virus pas geactiveerd als je een link of bijlage aanklikt?
Het is niet gevaarlijk als je op een e-mail zelf klikt. Het virus wordt pas geactiveerd als je op een bijgevoegde link of bijlage klikt.

Mogen bijlages en links uit interne e-mail worden geopend?
Ja, bijlages en links uit een interne e-mail mogen geopend worden.

Welke systemen liggen er allemaal uit?
Alle diensten die gebruik maken van en naar het internet liggen eruit. Denk aan internet, MEOS, YouForce, Secureweb, Securemail en Telewerken. We zijn hard bezig om de internetfunctionaliteit weer gefaseerd vrij te geven. Dat betekent dat sommige diensten snel weer zullen werken.