Gehackt! Wat nu?

Je zorgorganisatie is gehackt. Wat nu? Is de situatie ernstig? Zijn de hackers nog aanwezig op het netwerk?

Dit document bevat een globaal stappenplan voor iedereen in de organisatie om je op weg te helpen in geval van een hack. Je kunt dit gebruiken voor communicatie en aanpassen naar je eigen organisatie. Dit document beschrijft de grote lijnen voor actie, dit kan verschillend zijn al naar gelang zaken zijn uitbesteed aan leveranciers. Pas dit aan naar gelang de situatie en afspraken met leveranciers in je eigen organisatie.

Stappenplan

1.In alle situaties geldt: blijf kalm! Adrenaline is goed, maar paniek en stress zijn in zo'n situatie als olie op het vuur.

2.Laat de gehackte computer aan staan. Dit in verband met mogelijke sporen en aanwijzingen voor digitaal forensisch onderzoek.

3.Verbreek wel de netwerkverbinding van de computer om ervoor te zorgen dat hackers niet meer bij de computer kunnen en dat de computer ook niets kan verspreiden naar in het netwerk. (Bij een virtuele server kan de netwerkadapter worden losgekoppeld in het instellingenscherm)

4.Als er vermoeden is dat meerdere computers besmet zijn; zet de automatische back-ups uit. Bij ransomware of virussen kunnen bestanden aangetast zijn en zullen besmette/versleutelde bestanden naar de back-up worden weggeschreven.

5.Gooi niets weg en draai op deze computer geen (nieuwe) virusscanner die mogelijk aanwijzingen kan verwijderen.

6.Neem contact op met je CISO en informeer de betrokken manager en FG als dat nog niet is gebeurd.

7.Bel eventueel met Z-cert (033-7370609) om het incident te melden en te horen of er vergelijkbare incidenten spelen bij andere organisaties. (Melden kan ook als je geen lid bent)

8.Open een logboek waarin alle acties tijdens de crisis worden genoteerd.

9.Stel logfiles van firewall en Active Directory (eventlog) veilig op een externe mediadrager (Als kopie; niet verplaatsen).

10.Stel de bestuurder/directeur op de hoogte van de hack als dit nog niet is gebeurd, zodat besluitvorming kan plaatsvinden. Mogelijk moeten er systemen en/of werkzaamheden stilgelegd worden waardoor het incident de zorg of andere werkzaamheden raakt.

11.Formeer een crisisteam. De stappen die vanaf nu gezet worden kunnen dienstverlening raken. Ook is het mogelijk dat de hack of de gevolgen ervan impact zullen hebben op de eigen bedrijfsvoering of die van (keten)partners. Daarom bevat het crisisteam minimaal:

- de CISO als incidentmanager
- privacy officer
- technisch specialist / beheerder
- vertegenwoordiger van het management
- vertegenwoordiger van de zorg/dienstverlening
- communicatieadviseur
- de Functionaris Gegevensbescherming (FG)

12.Je staat nu voor een keuze; zelf het incident verder onderzoeken of een extern digitaal forensisch onderzoeksbedrijf inschakelen.

- Het voordeel van een extern digitaal forensisch onderzoeksbedrijf is up-to-date technische kennis en ervaring, specifieke expertise, specialistische apparatuur en extra handjes die gespecialiseerd de gemeente kunnen helpen met het opsporen en bepalen van reikwijdte van de hack.
- Kies je ervoor om het incident zelf verder te onderzoeken. Aarzel dan niet om toch een externe partij in te schakelen als je merkt dat het incident groter of complexer is dan gedacht.

13.Geef regelmatig instructies aan de servicedesk over hoe te communiceren en ook aan het klantcontactcentrum en de receptionisten als klanten last hebben van de hack. Lopen de betrokkenen een verhoogd risico dan moeten zij over het risico en voorval worden geïnformeerd.

14. Doe aangifte bij de politie en vraag specifiek naar een digitaal rechercheur.

15. Bij een grote hack kan het verstandig zijn om alle wachtwoorden van alle gebruikers, serviceaccounts, systeembeheerders te wijzigen. Denk zorgvuldig na over de communicatie met alle gebruikers, ook degene die (bijvoorbeeld vanwege vakantie) afwezig zijn.

16. Doe een (voor)melding bij de Autoriteit Persoonsgegevens na analyse van getroffen data. De (voor)melding moet binnen 72 uur na ontdekking van het incident zijn gedaan. Je kunt deze later aanpassen na nadere analyse van het incident.

17. Evalueer het incident; inventariseer lessons learned om een dergelijk incident in de toekomst te voorkomen. “Never waste a good incident!” En deel het incident met de geleerde lessen met collega-organisaties zodat je collega’s ook nadere stappen kunnen ondernemen.