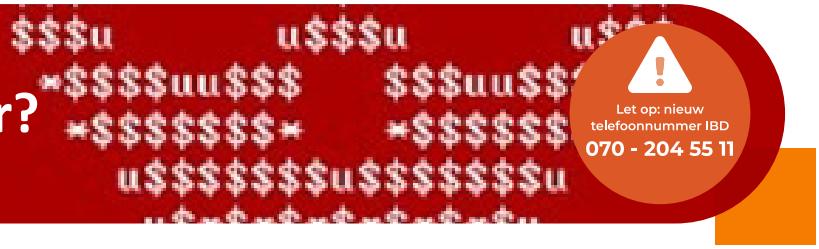
Gehackt, hoe nu verder?



Een gemeentelijke IT component (server/PC/firewall) is gehackt. Mogelijk is de situatie ernstig? Moet u zich zorgen gaan maken? U weet nog niet hoe groot de hack is, wanneer deze is begonnen en of de hackers nog aanwezig zijn op het netwerk. Ook blijkt dit scenario niet in het crisisplan voor te komen… Wat nu? Dit document bevat een globaal plan van aanpak om u op weg te helpen in geval van een hack. Aarzel niet om contact op te nemen met de IBD.

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 ten behoeve van digitaal forensisch onderzoek.
3. Verbreek de netwerkverbinding van de computer om ervoor te zorgen dat hackers niet meer bij de computer kunnen en dat de computer ook geen andere componenten in het netwerk verder kan verspreiden. Bij een virtuele server kan de netwerkadapter los worden gekoppeld in het instellingenscherm.
4. Gooi niets weg en draai op deze computer geen (nieuwe) virusscanner die mogelijk aanwijzingen kan verwijderen.
5. Neem contact op met de CISO van je gemeente en informeer de betrokken manager en FG.
6. Bel met de IBD (070 - 204 55 11) om het incident te melden en te horen of er vergelijkbare incidenten spelen bij andere organisaties.
7. Open een logboek waarin u alle acties tijdens de crisis noteert.
8. Indien er vermoeden is dat meerdere computers met ransomware besmet zijn; zet de automatische back-ups uit. Bij ransomware kunnen er diverse bestanden reeds aangetast zijn en zullen besmette/versleutelde bestanden naar de back-up worden weggeschreven.
9. Stel logfiles van firewall en Active Directory (eventlog) veilig op een externe mediadrager (kopieer bestanden; niet verplaatsen)
10. Stel de gemeentesecretaris op de hoogte van de hack zodat op een later moment besluitvorming snel kan plaats vinden. Mogelijk moet de dienstverlening stilgelegd worden bij een groot incident waardoor het incident de gemeentelijke dienstverlening raakt.
11. Formeer een crisisteam *afhankelijk van de grootte van het incident*. Bij een klein incident volstaat een klein team van specialisten. Maar een groter incident raakt de dienstverlening en bedrijfsvoering. Daarom bevat het crisisteam voor een groter incident minimaal:
    - vertegenwoordiger van het management als voorzitter
    - vertegenwoordiger van business/dienstverlening
    - de CISO als incidentmanager
    - technisch specialist / beheerder
    - communicatieadviseur
    - privacy officer
12. *Keuze*: De gemeente staat nu voor een keuze; zelf het incident verder afhandelen en onderzoeken of externe specialisten inschakelen.[1]
    De voordelen van een externe specialist zijn 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.[2]
    Indien er gekozen wordt om het incident zelf verder af te handelen of te onderzoeken is het verstandig om deze keuze op een later moment te nogmaals te bezien indien het incident groter of complexer is dan initieel bedacht.
13. Denk aan interne en aan externe communicatie. Geef regelmatig instructies aan servicedesk over hoe te communiceren. Indien ook de dienstverlening van de gemeente is betrokken, informeer dan ook het KCC. Indien u veel vragen van buiten verwacht: richt dan een vaste pagina in op de website met updates over het incident. De IBD kan adviseren over communicatie en woordvoering, aarzel niet om contact op te nemen op telefoonnummer 070 – 204 55 11.[3]

Tips en aanwijzingen

- Controleer firewall logs en netwerkverkeer. Wanneer, van waar naar waar, hoeveel en welk type netwerkverkeer heeft er plaats gevonden dat mogelijk in verband staat met de hack. Probeer verbanden te leggen in tijdstippen en het vreemde verkeer, dan kan worden achterhaald hoe de hackers zijn binnengekomen en vanaf wanneer. Noteer belangrijke tijdstippen van dit verdachte netwerkverkeer en gebruik deze voor onderzoek op logfiles en eventlog.
- Verhoog monitoring en controle op de firewalls. Pas toegangsregels aan (whitelisting van toegestane verbinding en blacklisting van verdachte verbindingen).
- Controleer de gebruikersaccounts in Active Directory. Zijn er nog nieuwe accounts bijgekomen die niet verklaard kunnen worden; bijvoorbeeld door deze te vergelijken met nieuwe medewerkers. Daarnaast moet worden gezocht naar accounts die verhoogde systeemrechten hebben gekregen; zijn beheeraccounts aangepast of gewijzigd? De Domain Controller is één van de meest waardevolle doelen voor een hacker.

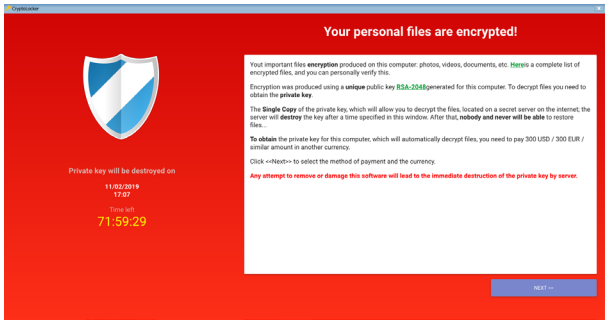
- Mogelijk zijn hackers al langer actief op het netwerk. Inventariseer of er in de afgelopen periode vreemde incidenten zijn geweest die mogelijk verband hebben met de hack. Denk hierbij aan problemen met de back-up omgeving, storage omgeving of niet gedocumenteerde wijzigingen in DMZ-omgeving.
- Voer een Back-up / Restore test uit. De hackers kunnen systematisch back-ups hebben vernietigd waardoor dient worden vastgesteld of er nog een restore kan worden teruggezet. Mogelijk zijn er offline back-ups die nog niet aangetast zijn die gebruikt kunnen worden. Kan er vanaf een restore een systeem volledig worden teruggezet en zijn bestanden leesbaar? (Doe een steekproef).
- Bekijk de back-ups van de gehackte server(s) in een quarantaine omgeving. Met de gegevens uit de back-up kunnen verschillen worden gezocht tussen het moment dat de server nog niet gehackt was en de huidige gehackte server. Kijk bijvoorbeeld naar vreemde bestanden in C:\Windows\Temp of naar C:\Users.
- Onderzoek logfiles en Windows eventlogs. Zoek naar brute-force inlogpogingen, lokale accounts die aangemaakt zijn (met verhoogde rechten), vreemde accounts en vreemde inlogtijden. Als er 's avonds laat een beheerdersaccount actief is geweest terwijl er geen wijzigingen gepland stonden, kan dit een aanwijzing dat er een hacker actief was.
- Indien duidelijk is dat een gehackte computer middels RDP is overgenomen vanaf afstand kan de tool "RDP Cached Bitmap Extractor" gebruikt worden om zo het beeld dat de hacker als laatst met RDP-sessie heeft gezien te tonen.
- Scan de DMZ-omgeving. Doe een security scan op de externe IP-adressen van de gemeente door middel van een kwetsbaarheden scan en controle op openstaande services en netwerkpoorten.
- Schoon de gehackte server uiteindelijk niet door het virus te verwijderen, maar bouw de server volledig opnieuw op. Zorg bij het opbouwen van de server voor dat er alleen vertrouwde executables gebruikt worden en gebruik geen oude executables van de oude server.

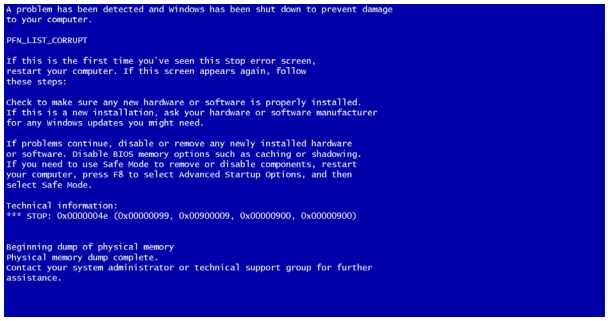
Nadere stappen:

- Indien het een grote hack betreft kan worden besloten 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.
- Doe aangifte bij de politie en vraag specifiek naar een digitaal rechercheur.

Doe een (voor)melding bij Autoriteit Persoonsgegevens na analyse van getroffen data; mogelijk later ook melden datalek of verlies van persoonsgegevens en dit een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. De (voor)melding moet binnen 72 uur na ontdekking van het incident zijn gedaan.

- Evalueer het incident; inventariseer lessons learned om een dergelijk incident in de toekomst te voorkomen. "Never waste a good incident!" De IBD helpt graag om deze lessen ook voor andere gemeenten op te halen.





Eindnoten

1 Zie ook de handreiking forensisch onderzoek van de IBD: https://www.informatiebeveiligingsdienst.nl/product/digitaal-forensisch-onderzoek/

2 Let wel op dat het externe onderzoek proportioneel is om zo kosten binnen de perken te houden.

3 De IBD stelt een leidraad Crisiscommunicatie beschikbaar aan gemeenten in geval van een incident, meer informatie via info@IBDGemeenten.nl

Let op: nieuw telefoonnummer IBD
070 - 204 55 11

Meer informatie

Meer informatie over onze dienstverlening vindt u in de andere factsheets van de IBD en op de website www.informatie-beveiligingsdienst.nl. De helpdesk van de IBD is te bereiken tijdens kantooruren van 9:00 tot 17:00 uur op het nummer 070 204 55 11 of via het e-mailadres info@IBDgemeenten.nl. De CERT van de IBD is 24x7 bereikbaar via 070 204 55 11 (instructies voor het piketnummer op de voicemail).