School CERT

Hulp bij een gecompromitteerd e-mail account

Laat ict werken **voor het onderwijs**

E-mailaccount gehackt, hoe nu verder?

Zie je wijzigingen in je e-mail account die je niet zelf hebt gemaakt? Zoals e-mails die als gelezen zijn gemarkeerd terwijl je ze nooit hebt geopend. Staan er e-mails in de verwijderde of verzonden mappen die je niet herkent? Heb je een wachtwoord resetmelding ontvangen die je niet hebt geïnitieerd? Hebben jouw contacten ongebruikelijke of verdachte e-mails ontvangen van jou? Weet je niet wat je nu moet doen?

Wanneer je e-mailaccount wordt gecompromitteerd, betekent dit dat iemand zonder jouw toestemming toegang heeft verkregen tot jouw account. Dit kan leiden tot verlies van privacy, diefstal van persoonlijke gegevens en zelfs tot financiële schade.

Dit document bevat een globaal plan van aanpak om je op weg te helpen in geval van een gecompromitteerd e-mailaccount.

Stappenplan

1. Wijzig het wachtwoord van het getroffen e-mailaccount. Bij voorkeur samen met de wachtwoordhints en beveiligingsvragen. Wachtwoorden worden vaak hergebruikt. Wijzig daarom het wachtwoord voor alle accounts waarbij dit wachtwoord gebruikt is.

2. Zorg dat de beheerder jou bij alle bestaande sessies uitlogt, omdat onbevoegden daar al ingelogd kunnen zijn met jouw wachtwoord.

3. Laat de beheerder van de mail voorziening het getroffen e-mailaccount blokkeren, zodat deze geen mail meer kan versturen.

4. Registreer het incident en begin met het vastleggen van de resultaten, de acties en besluitvorming. Dit kan bijvoorbeeld in een logboek of ticketingsysteem.

5. Start met het verzamelen van bewijslast voor later onderzoek door de politie of forensisch onderzoekers. Denk hierbij aan loggingsdata, (phishing)mails die verstuurd zijn naar contactpersonen, etc.

6. Start onderzoek naar hoe het account is gecompromitteerd en waarvoor het gebruikt is. E-mailaccount(s) kunnen op verschillende manieren worden gecompromiteerd. Zoals via phishing-aanvallen, malware, het gebruik van gegevens uit eerdere datalekken en credential dumps om credential stuffing-aanvallen uit te voeren, evenals het verzamelen van mogelijke accountinformatie van slachtoffers van sociale-mediaplatforms.

7. Bepaal wie het (forensisch) onderzoek uitvoert. Het onderzoek kan worden gedaan door eigen medewerkers, de ICT-leverancier of externe onderzoekers. Bijvoorbeeld van een Incident Response-bedrijf.

8. Als je vermoedt dat er sprake is van een malware-infectie, *laat de computer dan aanstaan*. Dit in verband met mogelijke sporen en aanwijzingen voor digitaal forensisch onderzoek.

9. Verbreek de netwerkverbinding van de computer. Zo zorg je ervoor dat hackers niet meer bij de computer kunnen en dat de malware zich niet kan verspreiden in het netwerk.

10. Controleer of er forwarding- of inbox rules zijn aangemaakt. Aanvallers creëren vaak regels voor het doorsturen van e-mail om gevoelige informatie te verzamelen en toegang tot de omgeving te behouden. Zelfs als het wachtwoord van een gecompromitteerd account opnieuw wordt ingesteld.

11. Controleer of er onbekende applicaties zijn geregistreerd. Aanvallers misbruiken OAuth-applicaties om toegang te krijgen tot het account van een slachtoffer zonder de inloggegevens van het slachtoffer te gebruiken. De gebruiker ontvangt een bericht om de applicatie met de gevraagde API-rechten te accepteren. Nadat de gebruiker accepteren heeft geselecteerd, heeft de aanvaller controle over het account van de gebruiker.

12. Als er malafide software is geïnstalleerd verwijder deze met malware tools, nog beter is het om het systeem opnieuw in te richten.

13. Informeer de privacyofficer en/of functionaris gegevensbeschermer van je school. Bepaal samen of er sprake is van een datalek en of er een melding gedaan moet worden bij de Autoriteit Persoonsgegevens. Doe dit in de eerste 72 uur na ontdekking van het datalek.

14. Informeer je contacten over de compromitering van je account, de genomen maatregelen en eventuele stappen die zij moeten ondernemen.

Tips en aanwijzingen

Onderzoek

Interview de getroffen gebruiker om details te verzamelen over de methode die mogelijk gebruikt is voor de compromise. Voorbeeldvragen:

- Heb je een verdachte e-mail ontvangen?
- Heb je jouw e-mailgegevens ingevoerd nadat je op een link hebt geklikt, of op een website die deze niet leek te accepteren?
- Heb je nieuwe software gedownload?
- Heb je per e-mail documenten ontvangen die je niet had verwacht?

Zoek in de mailbox van de getroffen gebruiker naar mogelijke phishing mails door te zoeken naar mails met een attachment of mails die urls bevatten naar externe sites.

Controleer inlogpogingen. Er worden inlogactiviteiten verwacht, vooral verdachte inlogpogingen, als een aanvaller toegang heeft gekregen of probeert toegang te krijgen tot de omgeving van het slachtoffer.

- *Verdachte inlogpogingen*: Inlogactiviteit vanaf ongebruikelijke locaties, systemen, user-agents of op afwijkende tijdstippen.
- *MFA-fouten:* MFA-fouten zijn een andere waarschuwing voor mogelijke kwaadaardige activiteiten. In sommige gevallen slaagt een aanvaller erin de inloggegevens van een gebruiker te bemachtigen en probeert de aanvaller in te loggen op het account, maar wordt de aanvaller tegengehouden met MFA (Multi-Factor Authenticatie).
- *Brute force:* Brute force-aanvallen veroorzaken veel foutieve inlogpogingen in een relatief kort tijdsbestek. Na het identificeren van een brute force-aanval, wordt aanbevolen om te bepalen of de aanval succesvol was. Dit bereik je door het observeren van een succesvolle login, voorafgegaan door een abnormaal aantal mislukte pogingen.

Voer een grondig onderzoek uit naar de oorsprong van de mail.

- E-mail artifacts: Afzender, onderwerp, body van de mail, e-mail header
- URL's/domeinnamen, DNS register, hosting partij, broncode van de phishing site
- Analiseer attachment via sandboxing tools en verzamel Indicators of compromise (IOC)
- Controleer of url's, domeinnamen, file hashes bekend zijn op verschillende threat intelligence services zoals virustotal.

Onderzoek waarvoor de aanvaller de gecompromitteerde accounts heeft gebruikt.

- Is er spam verstuurd?
- Zijn er specifieke mails verstuurd met gevoelige gegevens?
- Wordt binnenkomende e-mail doorgestuurd of naar de prullenbak gestuurd?
- Is het account gebruikt om verder het netwerk in te dringen?

Bepaal of er data is gelekt

Een van de grootste uitdagingen tijdens een BEC-onderzoek is het vaststellen welke e-mails of gegevens zijn benaderd, gekopieerd en/of geexfiltreerd door een aanvaller.
De benodigde (audit) logs kunnen ontbreken of niet volledig beschikbaar zijn omdat deze voor een beperkte tijd worden bewaard. Het is echter een goed uitgangspunt om aan te nemen dat een aanvaller toegang heeft gekregen tot alle e-mails binnen een gecompromitteerd account.
Kijk ook naar andere informatiebronnen zoals SharePoint, OneDrive, Google Drive, Shared mailboxen, netwerkschijven/file servers, etc. waar een aanvaller mogelijk ook toegang tot heeft gehad.

Rapportage en evaluatie

Rapporteer het incident en de genomen maatregelen aan het schoolbestuur en evalueer de effectiviteit van de manier waarop is omgegaan met deze situatie. Om lessen te trekken voor verbetering van toekomstige vergelijkbare incidenten.

Laatste update 02-10-2024

Voor ondersteuning: support@kennisnet.nl / 0800 321 22 33
Voor vragen over het School-CERT: cert@kennisnet.nl