5.1.2.e

Van: NP - Korpschef
Verzonden: vrijdag 8 november 2024 17:28
Onderwerp: Update datalek 8 november

Beste collega,

Niet onder reikwijdte

Ongeveer een maand geleden ontving je van mij een laatste update over de hack, waarbij de contactgegevens van politiemedewerkers zijn buitgemaakt. Het is na roerige weken ogenschijnlijk stiller rondom de hack, maar achter de schermen werken collega's nog altijd keihard. En dat blijven we doen. Enerzijds werken we aan het opsporingsonderzoek. Anderzijds nemen we maatregelen om ons nog beter te wapenen tegen cyberaanvallen. Dit laatste vraagt om alertheid van ons allemaal.

Stand van zaken opsporingsonderzoek
Team High Tech Crime van de Eenheid Landelijke Opsporing en Interventies (LO) doet onderzoek naar de sporen en de gebruikte werkwijze. Dit onderzoek is nog in volle gang en stap voor stap komen we meer te weten. In het belang van het onderzoek kunnen niet alle bevindingen gedeeld worden. Maar zodra dit wel kan, zullen we dat meteen doen. Zo werd eerder bekend dat zeer waarschijnlijk een statelijke actor verantwoordelijk is. Inmiddels weten we dat de daders vermoedelijk gebruik hebben gemaakt van een zogenoemde *pass-the-cookie*-aanval, waarbij een actieve sessie van een account wordt overgenomen met de bijbehorende rechten.

Op ons intranet is zojuist een artikel gepubliceerd waarin collega Stan Duijf van de LO hier uitgebreider over verteld. Er zijn op dit moment geen aanwijzingen dat er naast het adresboek andere gegevens zijn buitgemaakt.

Veiligheidsmaatregelen
Je merkt het nu misschien al bij het inloggen op bepaalde applicaties, dat er vaker om je wachtwoord wordt gevraagd. Dat je een wachtwoord moet aanpassen. Of dat er twee-staps-verificatie wordt toegepast. Dit zijn zichtbare maatregelen, maar hiernaast nemen we ook maatregelen waar je niets van merkt. We monitoren continu. Maar cyberveiligheid is een gezamenlijke verantwoordelijkheid. Onlangs heb je een mail ontvangen met een link naar de verplichte e-learning 'Ben jij Altijd Alert?' - Goud. Ik kan me goed voorstellen dat je ook andere, belangrijke dingen te doen hebt. Toch vraag ik je met klem om hier tijd voor vrij te maken. Je levert een belangrijke bijdrage aan onze weerbaarheid door voor het einde van het jaar deze e-learning te doen.

Tot slot, we proberen als organisatie en samen met al onze leidinggevenden om extra oog te hebben voor de zorgen die er leven. Ik weet dat die er zijn en ook dat we de zorgen niet altijd helemaal weg kunnen nemen. Toch is het belangrijk dat je er niet mee rond blijft lopen. Bespreek het met je leidinggevende of met elkaar. Ontvang je een verdacht bericht? Klik dan niet op een linkje, maar meld dit dan. Rechtsboven in Outlook zit de knop 'Phishing e-mail melden'. Op je werktelefoon kun je het bericht doorsturen naar 5.1.2.i @politie.nl Verdachte berichten lijken vaak urgent en afkomstig van een betrouwbaar iemand, maar deze persoon vraagt om ongebruikelijke informatie. Of de afzender vraagt je iets te downloaden of om op een link te klikken. In de e-learning leer je meer over de verschillende manieren waarop hackers jouw gedrag proberen te manipuleren met *social engineering*. Hoe beter we dit doorzien, hoe beter we onszelf kunnen beschermen.

Met vriendelijke groet,

Janny Knol
korpschef