5.1.2.e

Van: NP - Korpschef
Verzonden: dinsdag 27 mei 2025 10:30
Onderwerp: Nieuwe ontwikkelingen m.b.t. datalek (september 2024)

Beste collega,

De hack die onze organisatie vorig jaar september trof, heeft veel teweeggebracht. In een eerdere mail beloofde ik je te informeren over belangrijke ontwikkelingen.

We hebben eerder al gecommuniceerd dat er een statelijke actor achter de hack zat, met andere woorden: een ander land of daders in opdracht van een ander land. Inmiddels is door de inlichtingendiensten vastgesteld dat achter de hack een Russische hackersgroep zit – LAUNDRY BEAR – die dat zeer waarschijnlijk met steun van de Russische staat doet. Ze hebben vooral interesse in krijgsmachten, overheden, defensie(toe)leveranciers, sociaal-maatschappelijke organisaties en IT- en digitale dienstverleners.

Hoewel dit niet voor iedereen als een verrassing komt, kan ik me goed voorstellen dat dit iets doet met je gevoel van veiligheid. Weet dat onze collega's van onder andere het Security Operations Center (SOC), verantwoordelijk voor onze digitale veiligheid, meteen na de hack extra maatregelen hebben genomen. Deze nieuwe informatie helpt uiteraard om nog beter voorbereid te zijn op cyberaanvallen.

Het rapport over wie er achter de hack zit en hoe zij te werk gaan, wordt straks door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) gepubliceerd. Opsporingsonderzoek van onze eigen collega's van het Team High Tech Crime (THTC) ondersteunt deze bevindingen. Hoe dat is gegaan? Daarover lees je zometeen meer op BluePortaal.

Servicepunt
Bij die hack in september 2024 zijn zakelijke contactgegevens buitgemaakt. Toen, maar ook in vervolgonderzoek, hebben we niet kunnen vaststellen dat er meer gegevens gestolen zijn. Maar mocht je nog vragen of zorgen hebben en dat begrijp ik heel goed, dan kun je op meerdere plekken terecht. Uiteraard bij je leidinggevende of bij het speciale servicepunt, via 5.1.2.i (intern verkort: 5.1.2.i) of 5.1.2.i @politie.nl. Daarnaast is er ook op BluePortaal veel te lezen over wat je zelf kunt doen om beter voorbereid te zijn op cyberaanvallen of wat je moet doen als het dan toch gebeurt.

Iedere organisatie kan worden geraakt door een cyberincident, sterker nog: Nederland wordt doorlopend geconfronteerd met cyberaanvallen, aldus de AIVD en de NCTV. Met de NAVO-top in het vooruitzicht is een logische vraag of de huidige informatie daarop van invloed is. Maar cyberaanvallen waren al één van de scenario's waar we rekening mee houden. Want ook vorige NAVO-toppen kregen daarmee te maken. Dus vraag ik elke collega extra alert te zijn. En wat we nu weten over deze groep en hun werkwijze, helpt ons en ook andere organisaties de weerbaarheid te vergroten.

Wat je nog meer zelf kunt doen, blijft onveranderd: wees alert op phishingmails of verdachte berichten en telefoontjes. Vermoed je dat je zo'n mail hebt gehad, meld het dan. Rechtsboven in Outlook zit de knop 'phishing e-mail melden' en op je werktelefoon kun je het bericht doorsturen naar 5.1.2.i @politie.nl. En als je dat nog niet hebt gedaan, dan vraag ik je de e-learning Ben Jij Altijd Alert 2025 te doen. Niet alleen verplicht, maar ook heel verhelderend.

Dank aan iedereen die hier achter de schermen enorm hard aan heeft gewerkt, in het bijzonder de collega's van het Team High Tech Crime. Jullie hebben een 'huzarenstukje' geleverd.

Met vriendelijke groet,

Janny Knol
korpschef