Q&A webinar: Lancering vernieuwde Leidraad Cybersecurity

Tijdens het webinar was te weinig tijd om antwoord te geven op twee vragen. Die vind je hieronder beantwoord:

1. Wat moet je doen als het e-mailadres van een medewerker betrokken blijkt te zijn bij een datalek of hack?

Als een e-mailadres van een medewerker opduikt in een datalek, bijvoorbeeld via een melding van Have I Been Pwned of een alert vanuit jullie beveiligingssoftware, dan is snel en gestructureerd handelen belangrijk. Het gaat er niet alleen om het account te beveiligen, maar ook om te begrijpen wat er precies is gelekt en wat de risico's zijn voor de organisatie.

Stap 1 is het direct beveiligen van het account. Laat de medewerker het wachtwoord wijzigen van het betrokken e-mailadres, en ook van alle andere accounts waar hetzelfde wachtwoord werd gebruikt. Stel daarna tweefactorauthenticatie (2FA) in als dat nog niet het geval is.

Stap 2 is onderzoeken wat er is gelekt. Gaat het om een extern platform (zoals een webshop of nieuwsbrief-tool) of om een account dat direct toegang geeft tot systemen van de organisatie? Die tweede categorie vraagt om meer actie.

Stap 3 is beoordelen of er meldplicht geldt. Onder de AVG ben je als organisatie verplicht een datalek binnen 72 uur te melden bij de Autoriteit Persoonsgegevens als er persoonsgegevens zijn betrokken en het risico voor betrokkenen niet verwaarloosbaar is. Dat geldt ook als het lek bij een externe partij (bijvoorbeeld een leverancier) is ontstaan maar jouw medewerkers- of relatiedata bevat.

Stap 4 is intern communiceren. Zorg dat de IT-verantwoordelijke en de directie op de hoogte zijn. Als er reden is om aan te nemen dat het account is misbruikt voor phishing naar contacten van de organisatie, informeer dan ook die contacten.

Ten slotte: leg vast wat er is gebeurd, welke stappen zijn gezet en wat de uitkomst was. Dit is niet alleen goed voor de interne leerervaring, maar ook noodzakelijk voor de verantwoording richting toezichthouders.

2. Zien jullie ook risico's van aanvallen door statelijke actoren? Sommige NGO's zijn actief op politiek gevoelige terreinen, zoals mensenrechten.

Ja, dat risico is reëel, en het verdient een eerlijk antwoord. Organisaties die actief zijn op politiek gevoelige terreinen, zoals mensenrechten, vrijheid van meningsuiting, journalistieke ondersteuning of humanitaire hulp in conflictgebieden, behoren wereldwijd tot de doelwitten van statelijk gesponsorde cyberoperaties. Dit is geen theoretisch risico: internationale organisaties als Amnesty International en Human Rights Watch hebben dit in de praktijk ervaren.

Wat maakt NGO's kwetsbaar voor statelijke actoren? In de eerste plaats de aard van het werk: contactgegevens van activisten, bronnen of begunstigden in risicolanden zijn waardevolle informatie. In de tweede plaats de organisatiestructuur: veel NGO's werken met vrijwilligers, tijdelijke medewerkers en externe partners, wat de digitale perimeter groter en minder beheerst maakt. In de derde plaats de middelen: de beveiligingsvolwassenheid blijft bij veel goede doelen achter bij de dreiging waar ze aan blootstaan. Statelijke actoren onderscheiden zich van reguliere cybercriminelen door hun geduld, middelen en doelgerichtheid. Ze zijn niet altijd uit op financieel gewin, maar op informatie, beïnvloeding of sabotage. Denk aan spearphishing gericht op specifieke medewerkers, het compromitteren van communicatiekanalen of het in kaart brengen van netwerken van contactpersonen.

Wat kun je doen? Volledig beschermd zijn is niet realistisch, maar de weerbaarheid is wel degelijk te vergroten. Belangrijke maatregelen zijn: sterke authenticatie op alle accounts, bewustzijn bij medewerkers over gerichte phishing, versleutelde communicatie voor gevoelige uitwisseling, en een duidelijk beleid over wat wel en niet via reguliere e-mail mag worden gedeeld. Daarnaast is het verstandig om bewust na te denken over welke informatie in welke systemen staat en wie daar toegang toe heeft. Niet alle gegevens hoeven centraal opgeslagen te zijn, en minimale dataverzameling is zowel een AVG-principe als een beveiligingsmaatregel.

Voor organisaties die structureel actief zijn op politiek gevoelige terreinen adviseren wij een specifieke risicoafweging te maken, ook als de algehele volwassenheid op orde is. De dreigingscontext is dan een categorie apart.