Beantwoording vragen PvdA 13 september 2023

Onderstaand beantwoorden wij de gestelde vragen door PvdA. Op 23 november staat er een informatieve raadsbijeenkomst gepland met als thema informatieveiligheid.
Tijdens die bijeenkomst kunnen we dieper ingaan op gestelde vragen.

In de media is te lezen dat het aantal hack-pogingen en datalekken toeneemt. Ook de overheid is steeds vaker slachtoffer.

1. **Zou u een overzicht kunnen geven van het aantal hackpogingen van de afgelopen jaren? Bij ons en onze direct partners (buurtplein, buha etc)**

De fysieke en digitale omgeving waarin wij werken wordt dagelijks beproefd. Als u vraagt om het aantal hackpogingen en datalekken richten wij ons in deze beantwoording op onze digitale omgeving. Iedere dag opnieuw zijn er pogingen van derden om in te breken op onze ICT-omgeving. Deze pogingen zijn zowel gericht op daadwerkelijk inbreken in de technische ICT-systemen (het echte hacken), als op bijvoorbeeld phishing, omdat deze actie vaak ook tot doel heeft om toegang te krijgen tot informatie van anderen

Omdat er dagelijks pogingen worden ondernomen wordt dit risico gebaseerd geregistreerd. Kwetsbaarheidsmeldingen komen vaak binnen via de Informatiebeveiligingsdienst (IBD), in afstemming met het Nationaal Cyber Security Centrum (NCSC). Deze kwetsbaarheidsmeldingen krijgen een risico afweging mee. Hoge risico meldingen worden bijgehouden.

Daarnaast zijn er inbreuken die vanuit de eigen organisatie worden gemeld. Dit kan een beveiligingsincident zijn en/of een datalek, als het gaat om persoonsgegevens.

Deze laatst genoemde groep van inbreuken wordt geregistreerd en elke kwartaal gerapporteerd. Op dit moment wordt nagedacht om deze rapportage aan te vullen met de registratie over de eerste groep inbreuken.

2. **Zijn er ook pogingen succesvol geweest en wat is er toen gedaan? Hebben we de afgelopen jaren geld betaald aan ransom-ware?**

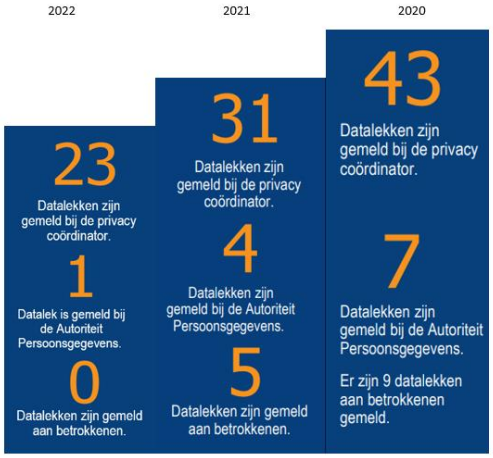
We verbeteren continu door acties op zowel het terrein van mens, techniek en organisatie. De beveiliging van onze ICT-infrastructuur bestaat uit verschillende lagen met daarbij horende proactieve en reactieve acties. Allemaal met als doel de ICT-infrastructuur veilig te houden. Veelal komen hack-pogingen niet door een eerste laag heen. Een enkele keer gebeurt dit wel; bv. door malware welke niet wordt opgemerkt. We zien dat de lagen daarna en de proactieve en reactieve acties hierop alsnog de hack-poging detecteren en verhinderen.

We hebben de afgelopen jaren geen geld betaald aan ransomware en adviezen die vanuit de experts (in en extern) worden gegeven zullen ook zijn om niet over te gaan op betaling.

3. **Is er ook een overzicht van datalekken van de afgelopen jaren?**

Er is een overzicht van alle datalekken. Zoals gezegd wordt dit allemaal geregistreerd en volgt elk kwartaal een rapportage richting het MT en de betrokken wethouder. Jaarlijks volgt een abstracte weergave van het aantal datalekken in de toetsing van de Functionaris Gegevensbescherming (FG). Die wordt ook jaarlijks aan u als mededeling aangeboden.

Als we kijken naar een overzicht in aantallen van de afgelopen 3 jaar dan neemt het aantal niet toe maar juist af.



4. **Mocht het nog niet zo zijn, zou het een idee zijn om jaarlijks bij bijvoorbeeld de begroting bovenstaande standaard te rapporteren?**

Zoals aangegeven ontvangt u jaarlijks al de informatie over datalekken. Mocht u andere zaken wensen dan horen wij dit graag.

Tijdens in de informatieve raad van 23 november kunnen we hierbij stil staan.

Het zal dan wel gaan om achteraf rapporteren in bijvoorbeeld jaarrekening en niet vooraf in de begroting.

5. **Hebben we beleid op het gebied van ransomware, hackpogingen etc?**

Recent is het nieuwe informatieveiligheidsbeleid vastgesteld. Daarnaast werken we met

- *Bedrijfscontinuïteitsplan met draaiboeken omtrent incident response en ransomware.*
- *Scenariokaarten*
- *Coordinated vulnerability disclosure*

Op 23 november is er een informatieve raad over dit onderwerp.
Graag bespreken we dan met u wat dit precies betekent.