SMT
Data zonder gedoe

USE CASE: DE BELASTINGDIESNT

# Van doelwit tot voorbeeld: hoe de Belastingdienst phishing- en smishingcampagnes de baas werd


## De situatie

De Belastingdienst kreeg te maken met een toenemende dreiging van phishing (via e-mail) en smishing (via sms). Burgers ontvingen misleidende berichten die leidden tot verwarring, reputatieschade en risico's voor de beveiliging van gevoelige gegevens.

Als organisatie met een publieke verantwoordelijkheid kon De Belastingdienst zich geen enkel incident permitteren. Er was behoefte aan een oplossing die snel verdachte patronen herkent en aanvallen proactief stopt.

## De uitdagingen

De uitdagingen lagen op drie fronten:

- **Voortijdige detectie:** phishing- en smishingcampagnes moesten in een vroeg stadium worden herkend
- **Schaalbaarheid:** het systeem moest miljoenen berichten per dag aankunnen
- **Vertrouwen beschermen:** burgers moesten erop kunnen rekenen dat hun persoonsgegevens veilig bleven en dat misleidende communicatie direct werd geblokkeerd

## De oplossing

**SMT** werkte nauw samen met **De Belastingdienst** en implementeerde een geïntegreerde oplossing op basis van **Splunk** en **Splunk SOAR**.

- **Splunk** dient als centraal monitoring- en analyseplatform dat realtime verdachte berichten detecteert
- **Splunk SOAR** zorgt voor geautomatiseerde workflows waarmee verdachte e-mails en sms'jes direct worden geïdentificeerd en geblokkeerd
- **Data** uit meerdere bronnen (zoals e-mailgateways, sms-kanalen en threat intelligence feeds) worden gecombineerd voor een volledig beeld

Dankzij deze aanpak kan De Belastingdienst phishing en smishing niet alleen sneller signaleren, maar ook direct neutraliseren met minimale tussenkomst van beheerders.

## Het resultaat

- ✓ **Snellere detectie** van verdachte berichten en aanvallen
- ✓ **Geautomatiseerde respons** die de belasting van securityteams verlaagt
- ✓ **Betere weerbaarheid** en versterkt vertrouwen bij burgers
- ✓ **Schaalbaarheid:** probleemloos verwerken van miljoenen berichten per dag

## De impact nu

De Belastingdienst beschikt over een robuust detectie- en responsplatform dat voortdurend meegroeit met nieuwe dreigingen. Burgers worden beter beschermd tegen frauduleuze berichten, incidenten worden sneller opgelost en het publieke vertrouwen blijft intact.

De effectiviteit van deze aanpak kreeg bovendien internationale erkenning tijdens Splunk.conf23 in Las Vegas, waar SMT samen met De Belastingdienst het project presenteerde. Daarmee werd zichtbaar hoe een Nederlandse overheidsinstantie niet alleen zijn eigen digitale weerbaarheid versterkt, maar ook wereldwijd als voorbeeld dient voor andere organisaties die worstelen met vergelijkbare dreigingen.

## Samenwerken aan digitale veiligheid

Met deze oplossing heeft de Belastingdienst een belangrijke stap gezet in het versterken van haar digitale weerbaarheid. Door Splunk slim in te zetten, processen te automatiseren en dreigingen proactief te monitoren, draagt de organisatie actief bij aan het beschermen van burgers tegen phishing- en smishing-aanvallen – en zet het een voorbeeld voor andere overheidsinstellingen.