orange™ Cyberdefense

Cybersecurity in de overheid

Inzichten en aanbevelingen uit Security Navigator 2025

Dreigingsbeeld overheid: van risico naar weerbaarheid

De overheid digitaliseert in rap tempo. Van digitale dienstverlening tot slimme steden en AI-gedreven besluitvorming, technologie versnelt de efficiëntie en bereikbaarheid van publieke diensten. Maar hoe digitaler de overheid, hoe groter het aanvalsoppervlak en daarmee het risico op cyberincidenten. Criminelen en statelijke actoren weten dat hier niet alleen waardevolle data te halen is, maar ook maatschappelijke ontwrichting teweeggebracht kan worden.

Orange Cyberdefense monitort wereldwijd cyberdreigingen. In dit document bundelen we onze belangrijkste bevindingen voor de publieke sector. Je vindt hier de meest relevante dreigingstrends, analyses en concrete adviezen om de digitale weerbaarheid van jouw overheidsinstelling te versterken.

Alle inzichten zijn gebaseerd op data en analyses uit de Security Navigator 2025.

De belangrijkste dreigingen voor de overheid

1. Cyberafpersing: ransomware blijft aan kop

Cyber Extortion (CyX) blijft de meest urgente dreiging voor overheidsinstellingen. Gemeenten, ministeries en uitvoeringsorganisaties worden frequent doelwit van aanvallen. In het afgelopen jaar steeg het aantal cyberafpersingsslachtoffers in de publieke sector met 31%, vooral door de groeiende agressie en morele grensvervaging bij aanvallers.

Waarom is de overheid een aantrekkelijk doelwit?

- Detectiedekking beperkt tot 41%.
- Significante reactietijd (38 uur).
- Kritieke afhankelijkheid van dienstverlening en publieke beschikbaarheid.

Advies: Investeer in proactieve detectie via gedragsanalyse, verkort de oplossingstijd (MTTR) met geautomatiseerde responsmechanismen en voer periodieke red teaming uit op vitale processen.

2. OT en Smart City-infrastructuur

Van verkeersregelinstallaties tot waterzuivering en energiemanagement; operationele technologie (OT) binnen gemeenten is steeds vaker geïntegreerd met IT-netwerken. Deze interconnectiviteit van IT- en OT-omgevingen zorgt voor nieuwe dreigingen.

In 2024 registreerden we 47 OT-gerelateerde incidenten:

- 16% hiervan betrof directe aanvallen op OT-functionaliteit (zogenaamde “Category 2” aanvallen), vaak uitgevoerd door geavanceerde actoren.
- 46% van deze geavanceerde OT-aanvallen resulteerde in directe manipulatie van fysieke processen (bijvoorbeeld verkeersregelsystemen).

Advies: Voer een gedetailleerde IT/OT-inventarisatie uit waarbij in kaart wordt gebracht welke systemen verbonden zijn. Segmenteer netwerken fysiek en logisch, en implementeer gespecialiseerde monitoring van industriële protocollen.

3. AI als aanvalsmiddel

AI-gebaseerde aanvalstechnieken winnen terrein, ook binnen de publieke sector. In 2024 werden deepfakes van overheidsfunctionarissen waargenomen in fraude- en phishingcampagnes. Ook worden taalmodellen ingezet voor geautomatiseerde spearphishing met AI-gegenereerde inhoud.

Voorbeelden uit 2024:

- Deepfake-video’s van burgemeesters ingezet voor fraude.
- Gerichte spearphishing met AI-gegenereerde inhoud.

Advies: Stel AI-governance-beleid op inclusief toegangscontrole en logging, test AI-systemen op misbruik (red teaming) en train personeel in het herkennen van AI-gedreven dreigingen.

4. Mobiele dreigingen: kwetsbaarheden op de werkvloer

Overheidsmedewerkers werken steeds vaker vanaf mobiele apparaten. Deze diversificatie van mobiele devices leidt tot een groter aanvalsoppervlak en verhoogde kwetsbaarheid. Mobiele aanvallen vormen een significant deel (33%) van dreigingen tegen eindgebruikers.

Aanvallers maken gebruik van:

- Sim-swapping en mobiele malware.
- Zero-click exploits.
- BYOD-omgevingen met onvoldoende beheer.

Advies: Implementeer Mobile Device Management (MDM), verplicht veilige netwerken (VPN), en ontwikkel trainingsmodules voor veilig mobiel gebruik.

Key onderzoeksdata voor de overheidssector

De overheidssector kende in 2024 een stijging van 31% in cyberafpersingsincidenten (CyX), met name binnen ondersteunende overheidsinstanties en de justitiële sector. Hacktivistische activiteiten, die vaak samenvallen met verkiezingen of geopolitieke gebeurtenissen, vormen een aanzienlijk risico. Deze aanvallen worden meestal uitgevoerd door externe actoren via hacking en misbruik van systemen.

Volgens de Security Navigator van is de gemiddelde oplossingstijd (MTTR 38) uur en ligt de detectiedekking op 41,43%. De Voice of the Customer (VOC)-cijfers, een kwetsbaarheidsmetriek op basis van harde data uit onze dienstverlening tonen gemiddeld 40,64 kwetsbaarheden per asset, waarvan kritieke issues gemiddeld 315 dagen blijven bestaan.

De Security Navigator benadrukt het belang van versterkte cybersecuritykaders, in het bijzonder om verkiezingssystemen en essentiële overheidsdiensten te beveiligen, gezien de wijdverspreide aanwezigheid van verouderde kwetsbaarheden.

Cy-X Victim ranking (Avg: 200)

Threat Detection: Mean time to resolve (Avg: 65h)

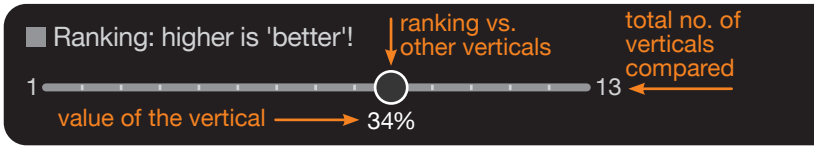
Cy-X Victim delta (Avg: +19%)

Threat Detection: Coverage (Avg: 37.5%)

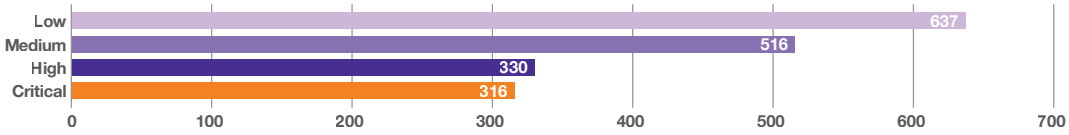
VOC: Findings per asset (Avg: 22.1 findings)

Threat Detection: True positives

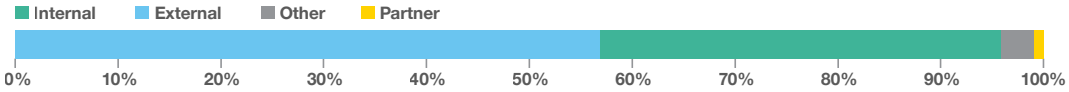
VOC: Total Vulnerability Score



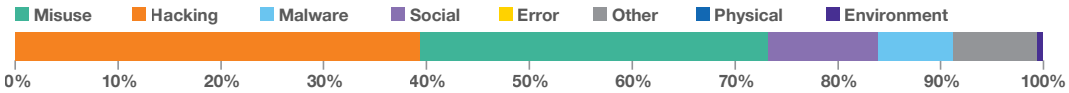
VOC: Finding age by severity (in days)



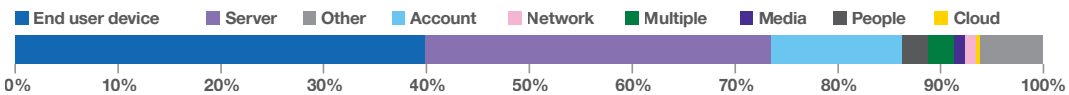
Threat Detection: Threat Actor



Threat Detection: Threat Action



Threat Detection: Impacted Asset



Concrete adviezen:

1. Zorg voor snellere detectie en respons

- Automatiseer incidentrespons met SOAR en verbeter escalatieprocedures in het SOC.
- Vergroot detectiecoverage door SIEM en EDR/XDR te optimaliseren en regelmatige Threat Hunting.
- Verminder false positives met AI en threat intelligence tuning.

2. Verminder kwetsbaarheden

- Verkort VOC-age (217 dagen gemiddeld).
- Implementeer risk-based patching en EPSS.
- Organiseer regelmatige pentests.

3. Beveilig OT- en smart city-infrastructuur

- Scheid OT van IT.
- Implementeer monitoring op industriële netwerken.
- Train operators in cyberfysieke risico's.

4. Implementeer Zero Trust-beleid

- Toegangsbeheer op basis van identiteit en context.
- Segmentatie van kritieke processen.
- Continue validatie van toegangsrechten.

5. Waarborg compliance en continue monitoring

- Automatiseer compliance-audits om te voldoen aan NIS2, GDPR en BIO.
- Implementeer 24/7 threat intelligence en monitoring via een MSSP of SOC.

Samen bouwen aan een veiligere digitale samenleving

De cijfers laten geen twijfel: de dreiging richting overheidsorganisaties groeit. Reactief beveiligen is niet genoeg. Alleen wie risico's begrijpt en er proactief op inspeelt, kan democratische processen, publieke diensten en burgervertrouwen waarborgen.

Bij Orange Cyberdefense staan we klaar om je daarbij te helpen. Als end-to-end cybersecurity dienstverlener ondersteunen we van strategie tot uitvoer en herstel.

Wil je sparren over de digitale weerbaarheid van jouw organisatie?

We begrijpen hoe de overheid werkt. Onze experts kennen de sector van binnenuit en weten wat er speelt, van de openbare ruimte tot aan de beleidstafel. Cybersecurity hoeft geen obstakel te zijn, maar kan juist zorgen voor efficiëntere processen en betere bedrijfsvoering. Ben je benieuwd hoe dit er voor jou uit kan zien? Plan dan vandaag nog een gesprek met één van onze experts.

www.orangecyberdefense.nl