Internet Society
Netherlands Chapter

ISOC NL Case Study “Digitale Soevereiniteit Beleidsmakers 2024”

inhoud

Introductie

In het kader van digitale bewustwording van zowel beleidsmakers als de internet gemeenschap ontwikkelt ISOC NL een casus over digitale soevereiniteit, gericht op de afhankelijkheid van Nederlandse overheden en kritieke beleidsmakers van buitenlandse e-maildiensten. Dit onderzoek, geïnspireerd door zorgen over Amerikaanse toegang tot deze gegevens, zal de implicaties voor digitale autonomie en privacy evalueren en mogelijke strategieën voor verbetering voorstellen.

1. Plan van Aanpak: Toetsen van Digitale Soevereiniteit

1.1. Doelstelling

Het primaire doel is het in kaart brengen en beoordelen van de digitale soevereiniteit van politieke partijen en ministeries, specifiek gericht op waar hun data gehost wordt en hoe dit hun digitale veiligheid en autonomie beïnvloedt.

2. Scope en Focus

- **Websites en Email Hosting**: Identificeer de hosting locaties van websites en emaildiensten van relevante politieke partijen en ministeries.
- **Beveiligingsmaatregelen**: Onderzoek de ingezette beveiligingsmaatregelen tegen bijvoorbeeld DDoS-aanvallen en spam.
- **Dienstenleveranciers**: Analyseer de afhankelijkheid van buitenlandse versus binnenlandse leveranciers voor cruciale digitale infrastructuur.

3. Methodologie

- **Data Verzameling**: Gebruik tools zoals traceroute, MxToolbox, en de diensten van Internet.nl om de fysieke locatie van servers en de gebruikte diensten te achterhalen.
- **Analyse van Veiligheidsrapporten**: Integreer veiligheidsrapporten van platformen zoals Internet.nl om een beeld te krijgen van de huidige veiligheidsstatus van deze entiteiten.
- **Historische Vergelijking**: Vergelijk huidige data met historische gegevens (indien beschikbaar) om veranderingen in hosting of beveiligingspraktijken te identificeren.

4. Communicatie en Bewustwording

- **Ontwikkeling van een Open Waarschuwingsbrief**: ISOC NL creëert met de Internet gemeenschap een document dat de bevindingen samenvat op een toegankelijke manier voor het brede publiek.
- **Samenwerking met Media**: ISOC NL werkt samen met journalisten en columnisten om de bevindingen te delen en bewustwording te creëren over digitale soevereiniteit.

5. Implementatie

- **Werkgroepen**: ISOC NL zet taken uit binnen de werkgroep Internet transparency van ISOC NL en andere belanghebbenden.
- **Feedback en Evaluatie**: ISOC NL organiseert sessies voor feedback op het voorlopige rapport.
- **Publicatie**: ISOC NL publiceert de bevindingen via diverse kanalen, inclusief sociale media en partner websites.

6. Vervolgacties

- **Aanbevelingen**: ISOC NL formuleert in samenwerking met de Internet gemeenschap concrete aanbevelingen voor politieke partijen en ministeries om hun digitale soevereiniteit te verbeteren.

- **Monitoring**: ISOC NL of een werkgroep stelt een periodieke review vast om de voortgang te monitoren en updates te geven over veranderingen in de digitale infrastructuur.

7. Partners en Hulpmiddelen

- ISOC NL identificeert partners binnen het veld die kunnen bijdragen aan technische expertise, historische data, of communicatiekracht.
- ISOC NL faciliteert de ontwikkeling van een toolkit of handleiding die organisaties kunnen gebruiken om hun eigen digitale soevereiniteit te beoordelen.

Dit biedt een gestructureerde benadering om de complexiteit rond de digitale aanwezigheid van politieke partijen en ministeries te adresseren, met een nadruk op veiligheid, transparantie, en autonomie.

8. Fictieve Casusomschrijving: De Partij voor Digitale Vooruitgang (PDV)

Om het bovenstaande plan van aanpak te verrijken, voegen we een casusomschrijving toe die illustreert hoe de toetsing van digitale soevereiniteit in de praktijk kan worden toegepast. Deze casus richt zich op de website van een fictieve politieke partij, de Partij voor Digitale Vooruitgang (PDV).

Achtergrond

De Partij voor Digitale Vooruitgang (PDV) is een politieke partij die zich richt op het bevorderen van digitale innovatie en technologie in het overheidsbeleid. Recent heeft de partij haar website vernieuwd om haar digitale aanwezigheid te versterken. Deze vernieuwing omvatte een verhuizing naar een nieuwe hostingprovider.

Uitdagingen

Na de lancering van de vernieuwde website ondervond PDV onverwacht hoge laadtijden en werd het doelwit van meerdere DDoS-aanvallen. Er rezen vragen over de keuze van de hostingprovider, de locatie van de servers, en de effectiviteit van de beveiligingsmaatregelen.

Doelstelling van de Toetsing

De toetsing is gericht op het evalueren van de digitale soevereiniteit van PDV door:
- De **fysieke locatie van de servers** te identificeren en te beoordelen hoe deze de websiteprestaties en toegankelijkheid beïnvloeden.
- De **beveiligingsmaatregelen** die zijn ingezet tegen DDoS-aanvallen te onderzoeken.
- De **afhankelijkheid van buitenlandse diensten** te analyseren en de impact daarvan op de digitale autonomie van PDV.

Methodologie

- **Data Verzameling**: Een traceroute-analyse wordt uitgevoerd om de route van de data naar de servers te volgen en de serverlocatie te bepalen. MxToolbox en Internet.nl worden gebruikt om inzicht te krijgen in de configuratie en beveiliging van de e-mailservers en de website.
- **Beveiligingsanalyse**: De gebruikte beveiligingsmaatregelen tegen DDoS-aanvallen worden geëvalueerd, met een focus op de effectiviteit van de maatregelen die door de hostingprovider zijn geïmplementeerd.
- **Analyse van Dienstenleveranciers**: Er wordt onderzocht of PDV afhankelijk is van dienstenleveranciers buiten hun controle, met name in het buitenland, en hoe dit hun digitale soevereiniteit beïnvloedt.

Resultaten en Aanbevelingen

De toetsing onthult dat de PDV-website gehost wordt op servers in een land met strenge privacywetten, wat positief is voor gegevensbescherming. Echter, de locatie draagt bij aan hogere laadtijden voor binnenlandse gebruikers. Bovendien blijkt dat de beveiligingsmaatregelen tegen DDoS-aanvallen onvoldoende zijn.

Op basis van deze bevindingen worden de volgende aanbevelingen gedaan:

- Overweeg hosting op locaties die zowel goede prestaties bieden aan binnenlandse gebruikers als sterke gegevensbeschermingswetten hanteren.
- Verbeter de beveiligingsinfrastructuur door samenwerking met gespecialiseerde diensten die robuuste DDoS-bescherming bieden.
- Verminder afhankelijkheid van buitenlandse diensten door te investeren in binnenlandse alternatieven waar mogelijk, om digitale autonomie te vergroten.

Deze casus illustreert het belang van een zorgvuldige afweging van hostinglocatie, beveiligingsmaatregelen, en de keuze van dienstenleveranciers om digitale soevereiniteit en veiligheid te waarborgen.

8.2 Digitale Soevereiniteit Analyse van BoerBurgerBeweging.nl

Op basis van de echte gegevens, kunnen we een gedetailleerde analyse uitvoeren van de digitale soevereiniteit van de BoerBurgerBeweging (BBB) met een focus op hun email en domeininfrastructuur. Deze informatie geeft inzicht in hoe BBB hun digitale aanwezigheid beheert en welke maatregelen ze hebben getroffen voor beveiliging en betrouwbaarheid.

Hosting en DNS Management

De DNS-records van boerburgerbeweging.nl worden beheerd door Cloudflare, wat aangeeft dat BBB gebruikmaakt van Cloudflare's diensten voor DNS management en waarschijnlijk ook voor beveiligingsdoeleinden zoals DDoS-bescherming en optimalisatie van de webperformance. Cloudflare is een Amerikaans bedrijf dat een uitgebreid netwerk van datacenters wereldwijd bezit, wat kan bijdragen aan snelle toegang tot de website van BBB vanuit verschillende locaties. Echter, de afhankelijkheid van een niet-Europees bedrijf roept vragen op over de digitale soevereiniteit en data-governance, gezien de mogelijke onderwerping aan buitenlandse wetgeving zoals de Amerikaanse Cloud Act.

Email Services

De MX-records van boerburgerbeweging.nl wijzen naar Google Apps (nu bekend als Google Workspace), wat betekent dat BBB Google's diensten gebruikt voor hun emailinfrastructuur. Dit toont aan dat BBB vertrouwt op een Amerikaanse provider voor hun emailcommunicatie, wat implicaties kan hebben voor de privacy en veiligheid van hun communicatie, gezien de data misschien opgeslagen en verwerkt wordt op servers buiten Nederland of de EU.

SPF en DMARC Records

BBB heeft zowel SPF (Sender Policy Framework) als DMARC (Domain-based Message Authentication, Reporting, and Conformance) records geïmplementeerd. De SPF-record bevat meerdere includes, wat betekent dat email namens BBB verstuurd kan worden vanaf servers van TransIP, Mailchimp, Google, en Seen.io. Dit is een goede praktijk voor emailverificatie en het tegengaan van spoofing.

De DMARC-policy is ingesteld op 'quarantine', wat betekent dat emails die niet voldoen aan de verificatie-eisen, naar de quarantaine worden verplaatst in plaats van direct te worden afgewezen. Dit is een veilige aanpak die helpt bij het identificeren en beheren van ongeautoriseerde emailverzending zonder legitieme emails volledig te blokkeren.

Analyse en Aanbevelingen

BBB heeft belangrijke stappen genomen om hun digitale aanwezigheid te beveiligen en de betrouwbaarheid van hun emailcommunicatie te verhogen. Echter, hun afhankelijkheid van niet-Europese dienstverleners voor zowel hun website als emailinfrastructuur stelt hen bloot aan potentiële risico's op het gebied van data governance en soevereiniteit.

De technische bevindingen die grondslag bieden aan deze vragen omvatten het niet volledig implementeren van IPv6, onvoldoende beveiligde HTTPS-verbindingen, en het niet instellen van alle aanbevolen beveiligingsopties voor de website van de BoerBurgerBeweging. Voor e-maildiensten werden DNSSEC tekortkomingen voor mailserverdomeinen en onvoldoende beveiligde mailserververbindingen zonder STARTTLS en DANE geïdentificeerd. Deze aspecten suggereren ruimte voor verbetering in digitale veiligheid en soevereiniteit, die de basis vormen voor bovengenoemde Kamervragen.

1. **Bekendheid met technische configuraties**: De website van BBB voldoet niet aan moderne internetadressering (IPv6) en heeft beveiligingsissues rond HTTPS.

2. **Verminderen afhankelijkheid van buitenlandse dienstverleners**: De bevindingen suggereren een heroverweging van de afhankelijkheid op diensten zoals Cloudflare en Google Apps, die buiten de EU zijn gevestigd.

3. **Essentieel onderdeel van nationale digitale infrastructuur**: De gesignaleerde beveiligingsissues benadrukken het belang van een veilige en soevereine digitale infrastructuur voor politieke entiteiten.

4. **Risico's en gevolgen afhankelijkheid niet-Europese technologie**: De tekortkomingen in IPv6 en HTTPS beveiliging tonen de risico's van afhankelijkheid op niet-Europese technologieën en diensten.

5. **Waarborgen privacy en veiligheid**: De onvolledige implementatie van DNSSEC en de beveiligingsconfiguraties suggereren dat verbeteringen nodig zijn om de privacy en veiligheid van data en communicatie te waarborgen.

6. **Voldoen aan Nederlandse en Europese normen**: De geïdentificeerde tekortkomingen duiden op noodzaak voor BBB om hun digitale infrastructuur te verbeteren om te voldoen aan de normen voor digitale veiligheid en privacy.

7. **Migratie naar Europese of Nederlandse dienstverleners**: De afhankelijkheid van buitenlandse dienstverleners en de beveiligingstekortkomingen bieden concrete aanleiding om de mogelijkheden voor migratie naar Europese of Nederlandse dienstverleners te overwegen.

Aanbevelingen voor de BoerBurgerBeweging kunnen onder meer zijn:
- Overwegen van Europese alternatieven voor DNS management en emaildiensten om beter in lijn te zijn met de Europese regelgeving omtrent data privacy (GDPR).
- Evalueren van de hosting- en serviceproviders op basis van hun naleving van de Europese normen en wetgeving.
- Continu monitoren en bijwerken van SPF en DMARC records om te verzekeren dat de emailbeveiliging up-to-date blijft en afgestemd is op de beste praktijken.

Deze analyse en aanbevelingen benadrukken het belang van digitale soevereiniteit en de noodzaak voor politieke bewegingen zoals de BoerBurgerBeweging om zorgvuldig hun digitale infrastructuur en diensten te kiezen, rekening houdend met zowel beveiliging als compliance met lokale en internationale wetgeving.

De BoerBurgerBeweging website scoorde 91% op Internet.nl met aanbevelingen voor verbetering, waaronder volledige IPv6-ondersteuning en verbeterde HTTPS-configuratie. De e-mailinfrastructuur scoorde 77%, waarbij verbeteringen nodig zijn in DNSSEC voor mailserverdomeinen en een veiligere mailserververbinding via STARTTLS en DANE. Beide tests toonden sterke punten zoals DNSSEC voor de domeinnaam, DMARC, DKIM en SPF configuraties voor e-mailauthenticiteit, en RPKI-validatie voor gerouteerde aankondigingen. Verbeterpunten betreffen vooral de uitbreiding naar moderne internetstandaarden en het verhogen van de beveiliging.

Voor meer details over deze resultaten, bezoek de volgende links op Internet.nl:
- [Website testresultaten](https://internet.nl/site/boerburgerbeweging.nl/2668438/)
- [E-mail testresultaten](https://internet.nl/mail/boerburgerbeweging.nl/1175562/)

In de uitgebreide casusomschrijving voor de BoerBurgerBeweging (BBB) zijn de website en e-mailinfrastructuur geëvalueerd met behulp van Internet.nl, waarbij de website een score van 91% en de e-mail een score van 77% behaalde. Verbeterpunten voor de website omvatten de volledige implementatie van IPv6 en het versterken van HTTPS-veiligheid. Voor e-mail worden verbeteringen aanbevolen in de DNSSEC-configuratie voor mailserverdomeinen en de beveiliging van mailserververbindingen met STARTTLS en DANE. Deze resultaten tonen aan dat BBB goed presteert op het gebied van digitale veiligheid en internetstandaarden, maar ook ruimte voor verbetering heeft, vooral in de adoptie van moderne internetprotocollen en beveiligingspraktijken.

Internet.nl is een initiatief dat helpt beoordelen hoe modern en veilig jouw internet is. Het kijkt naar website- en e-mailinstellingen om te zien of ze voldoen aan de nieuwste internetstandaarden. Protocollen zoals HTTPS, IPv6, DNSSEC, DMARC, DKIM, en SPF verbeteren de veiligheid en betrouwbaarheid van internetgebruik. HTTPS beschermt gegevens tussen websites en gebruikers, IPv6 zorgt voor meer internetadressen, en DNSSEC voorkomt omleiding naar valse websites. DMARC, DKIM, en SPF helpen e-mailbescherming door te verzekeren dat berichten echt zijn en niet vervalst.

Mogelijke Kamervragen aan de BBB-fractie

Gebaseerd op de casus van de BoerBurgerBeweging (BBB) en de informatie over hun digitale infrastructuur kunnen de Kamervragen omtrent SIDN als volgt worden herformuleerd gericht aan de BBB-fractie:

1. Bent u bekend met de technische configuraties en beveiligingsmaatregelen van de digitale infrastructuur van de BBB, waaronder de website- en e-maildiensten, zoals geëvalueerd door Internet.nl?

2. Heeft de BBB-fractie overwogen de afhankelijkheid van buitenlandse dienstverleners te verminderen om de digitale soevereiniteit en veiligheid te verhogen?

3. Deelt u de mening dat de digitale infrastructuur van een politieke partij, inclusief de website en e-maildiensten, een essentieel onderdeel is van de nationale digitale infrastructuur?

4. Hoe beoordeelt u de risico's en gevolgen van de afhankelijkheid van niet-Europese technologie- en cloudproviders voor de BBB's digitale infrastructuur?

5. Welke stappen onderneemt de BBB om de privacy en veiligheid van de data en communicatie binnen hun digitale domein te waarborgen tegen toegang door buitenlandse overheden?

6. Hoe zorgt de BBB ervoor dat hun digitale infrastructuur voldoet aan de Nederlandse en Europese normen voor digitale veiligheid en privacy?

7. Zijn er plannen of overwegingen binnen de BBB om te migreren naar Europese of Nederlandse dienstverleners om de digitale autonomie te vergroten?

Deze vragen richten zich op het belang van digitale veiligheid, privacy, soevereiniteit, en de afhankelijkheid van buitenlandse technologieën, en zijn relevant voor elke organisatie, waaronder politieke partijen zoals de BBB.

 | e-mail: bureau@isoc.nl . Koninklijke Bibliotheek, Prins Willem-Alexanderhof 5 (kamer i4.301) . 2595 BE Den Haag . Nederland |