Scan report

Target domain: Staatsbosbeheer

JAN FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC 2018

Initial list

staatsbosbeheer.nl

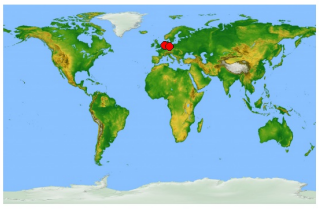
This list demarcates the scope, servers are added or removed by request

Amount of servers found

20

Server locations

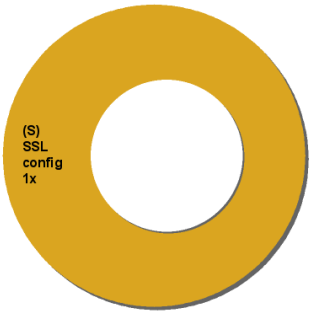
Netherlands 18
Germany 2



Based on geo-IP data. The physical location may deviate.

The inventory of the internet-domain is based on public information.

Security issues on servers



E-mail policy & blacklisting

Spam reputation | Prevention of phishing | Insight in abuse

The entire internet-facing environment is checked with a security quickscan.

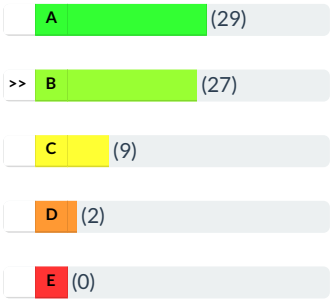
The most vulnerable server is monitoringt.staatsbosbeheer.nl

Overall security rating

B

A-Good
B-Sufficient
C-Doubtful
D-Below baseline
E-Vulnerable

Benchmark with sector 'Toezichthouders'



Amount of organizations per security rating. The arrow indicates the position of the own organization.

Trend

Overall security scores of Staatsbosbeheer in de past months.

Details of domain inventory

Network (name, owner, location)	IP-address	DNS-name	Security score
TRANSIP-COLO-865 Transip B.V. Colocation VLAN 865 Netherlands	80.69.65.0 - 80.69.65.255		
	80.69.65.40	service.staatsbosbeheer.nl	
AMAZO-ZFRA A100 ROW GmbH Germany	18.194.0.0 - 18.195.255.255		
	18.194.104.250	beeldverhaal.staatsbosbeheer.nl	100
NL-BIT-EVIDU-COLO-2 Evident Interactive BV Netherlands	213.154.250.192 - 213.154.250.255		
	213.154.250.217	staatsbosbeheer.nl	100
	213.154.250.217	www.staatsbosbeheer.nl	100
	213.154.250.217	kaart.staatsbosbeheer.nl	100
	213.154.250.217	beeldverslagoverijssel.staatsbosbeheer.nl	100
CJ2-CUST-TCN-SBB CJ2 Customer Staatsbosbeheer Netherlands	46.182.221.192 - 46.182.221.223		
	46.182.221.198	vpn.staatsbosbeheer.nl	100
	46.182.221.200	webmail.staatsbosbeheer.nl	100
	46.182.221.203	autodiscover.staatsbosbeheer.nl	100
	46.182.221.204	mail.staatsbosbeheer.nl	100
	46.182.221.206	mdm.staatsbosbeheer.nl	100
	46.182.221.207	eas.staatsbosbeheer.nl	100
	46.182.221.212	monitoringt.staatsbosbeheer.nl !	76 (S)
	46.182.221.213	geodata-a.staatsbosbeheer.nl	100
	46.182.221.213	geodata-t.staatsbosbeheer.nl	100
	46.182.221.213	geodata.staatsbosbeheer.nl	100
	46.182.221.220	webclient.staatsbosbeheer.nl	100
	46.182.221.221	webclient-t.staatsbosbeheer.nl	100
CJ2-CUST-INTRA-IT-2 Intra-IT subnet #2 Netherlands	5.22.248.64 - 5.22.248.127		
	5.22.248.100	millingerwaard.staatsbosbeheer.nl	100
AMAZO-ZFRA A100 ROW GmbH Germany	52.28.0.0 - 52.29.255.255		
	52.28.97.229	beeldverhaal.staatsbosbeheer.nl	100

Explanation domain inventory

What are the deliverables of the scan?
This is an automated discovery scan on the specified domain, supplemented by a security quickscan. It delivers:

- An overview of the (web)servers in a domain
- Insight in the hosting locations (own netwerk, ISP, cloud service provider)
- A security indicator per server: is additional investigation needed?
- A security benchmark in comparison with other organizations.

How does it work?
Based on one or a few website names, the scanner starts to search for related sites. These are found by using google searches, links on the website, portscans around identified websites, and other public sources. This leads to an overview of websites that presumably belong to the same organization, including their network location. The report contains an overview of all servers found, on the organization's network and other network ranges. By request, websites can be manually placed out-of-scope or in-scope, to improve the results.

In addition to the domain inventory, security checks are done for a few common vulnerabilities.

How is the security score calculated?
Each server is given a security score that is based on a dozen non-intrusive checks in the following categories:

- (P) Patch management - a (visible) lag in software versions
- (B) Blacklisted - presence on a blacklist of servers that distribute malware (not spam)
- (S) SSL/TLS-configuration - weak encryption, expired certificate, etc.
- (H) SSH-configuration - weak cryptokey
- (W) Webserver configuration - unsafe HTTP-methods or missing HTTP security headers
- (J) JavaScript library - vulnerable to XSS, suspicious content-server
- (C) Content Management System - lag in patches or not hardened properly
- (N) Nameserver configuration - zone transfer
- (D) Design issues - logon over plain-text connections, etc.

The security score is based on falsification: it is assumed that the server is secure, unless the opposite is proved. Every server starts with 100 points and each encountered vulnerability costs points. If a vulnerability can't be assessed, no points are lost.

Why is the security score useful?
The underlying idea is that with a few checks a quick indication is obtained of possibly vulnerable servers. The security score itself is no hard evidence but gives raise to further investigation. The logical follow-up is a full-blown security scan on a suspicious server. After that, the root cause of the vulnerability is known and it can be decided how to remediate this. Think about improvements in patch management, configuration management, tweaking the security baseline, etc. With these security metrics, the security manager is able to implement structural improvements in security where needed.

Green indicators from this quickscan does not mean that there are no vulnerabilities in a server. It only means that a few common security errors have not been found or could not be falsified. No server has been completely validated.

By repeating this check every month, trends become visible.

Disclaimer

Although this report has been created after careful research and testing, no guarantee can be given for its completeness nor for the actual risk level of the servers that are reported.

This quickscan is not a full-fledged security assessment. For a thorough assessment it is advised to execute a penetration test.

E-mail security details

Delivery not blocked by blacklists

It is checked if the mail servers of the domain are know to send spam.

Domain(s)	Mailserver	IP-adress	Blacklisting(s)
staatsbosbeheer.nl	mx1.staatsbosbeheer.nl	46.182.221.201	
staatsbosbeheer.nl	mx2.staatsbosbeheer.nl	46.182.221.202	

Detect spear-phishing

Of the core domain, the SPF-policy has been checked.

Domain	Name SPF-record	Finding	Finding details	Recommendation
staatsbosbeheer.nl	_customers.moreover.com	OK	Domain indicates the most probable mail servers	
staatsbosbeheer.nl	spf.mandrillapp.com	OK	Domain indicates the most probable mail servers	
staatsbosbeheer.nl	staatsbosbeheer.nl	OK	Domain defines a set of servers to send email	

Monitor fake senders (DMARC)

Of the core domain, the DMARC-policy has been checked.

Domain	Name DMARC-record	Finding	Finding details	Recommendation
staatsbosbeheer.nl	_dmarc.staatsbosbeheer.nl	No DMARC	DMARC is not implemented	Consider implementing DMARC at staatsbosbeheer.nl.

Explanation e-mail security

For hackers, e-mail is a succesful means to obtain passwords and distribute malware.

What's the problem?
A popular technique is 'phishing', where the user recieves an e-mail and is seduced to click on a link, open an attachment, etc. This fake-mail can look very genuine, especially if the sender address is that of a colleague or manager.
Many people don't know that the e-mail address that is included as 'sender' in the mail message has no relation at all with the person that actually sent the mail. They think that the sender name and address on top of the message is the real sender. However, for the hacker this is a free text field where he/she can fill in any e-mail address. What makes it worse is that the address of the real sender is not displayed to the user. This kind of phishing mail that is aimed to a specific group of persons is called spear-phishing.

What can you do against it?
To avoid abuse of e-mail adresses, a set of measures is available. Together, they facilitate in:

- Better recongnition of (spear-) phishing.
- Keeping sight on abuse of e-mail of your domain.
- Improvement of deliverability of your outbound e-mail.

In the rapport of the Internet-Security-Scan, these three aspects are given a score. The score is not limited to your own domain, but includes that of other mail domains that are important to the organization.
The NCSC (National Cyber Security Centre in the Netherlands) advises to implement SPF, DMARC and DKIM. These protocols are explained beneath.

Recognition of (spear-)phishing
The mail server can detect that mail is sent by a mail server that is not part of the sending domain. Consequently, the mail can be dropped or sent through with the label 'suspicious'.

- SPF (Sender Policy Framework)
  In the DNS-server, a list of mailservers is published that are allowed to send mail on behalf of this domain. In addition, a policy needs to be configured (block, mark as suspicious, pass-through). See OpenSPF.
- IDS (Intrusion Detection System)
  Scan incoming mail for suspicious senders and malicious content.
- AV (Anti-Virus) on the workspace
  In case that an end user clicks on something in a phishing mail, the AV-solution can detect and block this.
- Phishing tests
  Make users aware of phishing and train them in recognizing it.

Keep sight on abuse of mail in your domain
In order to get informed about the abuse of e-mail addresses of your domain, reports can be received from Internet Service Providers.

- DMARC (Domain-based Message Authentication, Reporting & Conformance)
  State in the DNS-server what report you'd like to receive. See DMARC.org.

Improving deliverability of your e-mail
Two things are important for deliverability: One is the level of confidence that the mail is sent by an authenticated mail server. The other important thing is that the mailserver is not known for sending spam.

- Monitor spam-blacklists
  A domain can get registered on a blacklist for several reasons. Check the cause and fix it.
- DKIM (DomainKeys Identified Mail)
  Digital signing of e-mail on behalf of the domain increases confidentiality in the sender.

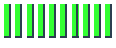
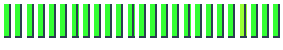
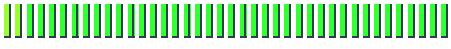
Appendix I. How to improve the security rating?

#	IP-adress	Hostname	Finding	Finding details	Recommendation
1		staatsbosbeheer.nl	Mail DMARC record	DMARC is not implemented	Consider implementing DMARC at staatsbosbeheer.nl.
2	46.182.221.212	monitoringt.staatsbosbeheer.nl	Certificate has expired.	sslExpireDate on 46.182.221.212:443 is 2015-03-28. Certificaat is issued for 'monitoringt.staatsbosbeheer.nl'.	Renew the server certificate on 46.182.221.212 (monitoringt.staatsbosbeheer.nl)
3	46.182.221.212		Old SSL version supported.	sslv3 is supported on 46.182.221.212:443.	SSLv2, SSLv3 and TLS1.0 are considered insecure. Make sure that the TLS-socket on only supports newer versions. Verify your configuration at ssllabs.com
4	46.182.221.212		Server supports WEAK ssl protocol(s).	WEAK ssl protocol(s) supported on 46.182.221.212:443.	Algorithms with short keys (such as MD5, RC4) are insecure. Make sure that only recommended algorithms and keylengths are supported on 46.182.221.212. See https://www.keylength.com/ for crypto standards. Verify your configuration at ssllabs.com

Checked on 20180118

Appendix II. Sector report

Security ranking of organizations in sector 'Toezichthouders'

Overall security rating	Organization	Security score of internet-facing servers (each block represents a server)	E-mail security score
A	Agentschap Telecom		
A	Nederlandse Voedsel- en Warenautoriteit		
A	Inspectie voor het Onderwijs		
A	Inspectie voor de Gezondheidszorg		
A	Inspectie Jeugdzorg		
A	Nationale Politie		
A	Erfgoedinspectie		
A	College voor de Rechten van de Mens		
A	Commissariaat voor de Media		
A	College voor de Toelating van Bestrijdingsmiddelen		
A	Kansspelautoriteit		
A	Nederlandse Emissie Autoriteit		
A	College Bescherming Persoonsgegevens		
A	Stimuleringsfonds voor de Pers		
A	Stichting Erkenningsregeling voor de Uitoefening van het Koeltechnisch Installatiebedrijf		
A	Verispect		
A	Stichting ter Exploitatie van Naburige Rechten (SENA)		
A	Stichting Kwaliteitscentrum Examinering		
A	Autoriteit Persoonsgegevens		
A	Landelijke Inspectiedienst Dierenbescherming		
A	Inspectie SZW (Arbeidsinspectie)		
A	Uitvoeringsinstituut Werknemersverzekeringen		
A	Nederlandse Algemene Keuringsdienst voor Zaaigoed en en Pootgoed van Landbouwgewassen		
A	Dienst voor het Kadaster en de Openbare Registers		

Overall security rating	Organization	Security score of internet-facing servers (each block represents a server)	E-mail security score
A	De Nederlandse Bank		🙂
A	Raad voor de rechtspraak		🙂
A	Geschillencommissie		🙂
A	Bureau Financieel Toezicht		🙂
A	Autoriteit Consument en Markt		🙂
B			🙂
B			🙂
B			🙂
B			🙂
B			😐
B			🙂
B			😐
B			😐
B			🙂
B			🙂
B			🙂
B			🙂
B			🙂
B			🙂
B			🙂
B			🙂
B			🙂
B			🙁
B			🙁
B			😐
B			🙁

Overall security rating	Organization	Security score of internet-facing servers (each block represents a server)	E-mail security score
B			
B			
B			
B			
B	Staatsbosbeheer		
B			
C			
C			
C			
C			
C			
C			
C			
C			
C			
D			
D			

Explanation of the footprint column: all the front-end servers of an organization are shown. Each block represents an internet-facing server, the color indicates its security score. A green block represents a server with no security issues, a yellow block is less secure and an orange or red block represents a server that needs immediate attention.