NETWORKING4ALL
SSL CERTIFICATES • DOMAIN NAMES • HOSTING

Networking4all

Security of personal data with participating political parties in Dutch parliamentary elections 2010

June 2010

Foreword

There is much to do about privacy. Whether on the Electronic Patient Dossier (EPD) or the Public transport smart card. The Dutch Personal Data Protection Act (WBP) is a hot issue and many parliamentary questions are made. One after the other party says that things are not safe enough and that it should be safer. In view of the parliamentary elections on Wednesday, June 9, 2010 it seemed interesting to Networking4all to test the websites of the participating parties.

The EPD may be in dispute, but are the sites of the political parties themselves safe and is the (sensitive) information from the citizens in safe hands? Indeed, political parties need to handle to the WBP, and therefore their websites as well.

Networking4all examined the websites of all eighteen political parties participating in the parliamentary elections on June 9. Of the known parties like PvdA and VVD to the young party Lijst 17 and the Piratenpartij. All sites ask for personal information. Thus, passwords, bank account numbers and Social Security numbers should be completed. For example at a member registration. Personal data should in all cases be secured.

This report describes the security of websites of political parties and how they handle the personal data of the visitor. We would certainly expect that the authoritative parties handle our data safely. But is that really the case?

Index

1 Introduction

1.1 The research

Networking4all is constantly concerned with the security of personal data on the web. Often, data is sent over an insecure connection and attackers (hackers) can intercept the information. The consequences for the victims of this form of Internet fraud can be significant. Because of this threat, the Dutch Data Protection Authority (CBP) recommends to use an SSL Certificate. This study aims to find out how carefully political parties use the Personal Data Protection Act.

The protection of personal data is legally obligatory in the Netherlands (see also section 1.4). Networking4all regularly examine to find out how serious this law is taken, whether or not related to current issues. This time the parliamentary elections. Purpose of these studies is to aware the society of the potential dangers on the web and to inform them about the safety.

You would expect that the political parties comply with the law. But is that true? Do the political parties in the Netherlands take the law seriously? Will they do respect the personal information of its visitors?

Accountability

Networking4all examine all eighteen political parties participating in the parliamentary elections of June 9, 2010.

For a representative research Networking4all examined all sites at various points. Such as possession of an SSL Certificate for being able to offer a secure method of sending (confidential) information. In addition, the websites are also checked for the existence of various interactive components such as a webshop, contact form and a login feature. Here, we looked whether the data are protected as they are completed. For example a bank-account number, social security numbers and/or a password. Also when for example the webshop is located on an external page. Finally, we checked if signing up for the newsletter is possible without the danger that cyber criminals can easily collect email addresses.

1.2 Who is Networking4all?

Networking4all offers solutions for digital security issues to society. Besides we simplify and centralize hosting and domain registrations. It is our passion to make society aware of and to offer solutions in online services and security in a quick and efficient way.

Networking4all has been an ambitious company already since its founding in 2000. Networking4all has the following mission: “To raise awareness to the society in a fast and targeted way and to offer solutions for online services and security.”

1.3 The importance of SSL

Networking4all mainly checks whether data is sent over a secure connection by using an SSL Certificate.

This is the method complies with the Personal Data Protection Act (WBP) and as the Data Protection Authority (CBP) advises. See also section 1.4.

SSL is used by millions of web sites to secure the Internet, including online purchases, financial transactions or sending personal data. This information remains confidential during transmission and cannot be read by others.

Web sites secured by SSL can be recognized by the closed padlock and the https:// in the address bar, as one can see, for example, on the login page of one's bank. An SSL Certificate is required for an SSL connection. A user can use an SSL Certificate to see who owns the site and who issued the certificate. There are several methods for the validation of SSL Certificates, namely domain validation (DV), organization validated (OV) and extended validation (EV).

An SSL Certificate is also very important for the identity of the site and its owner. It gives confidence. Visitors of the site know that their personal information is handled safely, and malicious persons may not ‘eavesdrop’.

Meaning

SSL stands for Secure Sockets Layer. The third version of SSL was the mainstay of Transport Layer Security (TLS), the current implementation of SSL. However, the name SSL is still used when it comes to securing the Internet connection.

Full coverage?

A website that does not use a secure connection can be intercepted. An SSL Certificate offers the most optimal protection, but can not give hundred percent guarantee. However, for an user an SSL Certificate is at this time the most useful way to check how a site handles (personal) data and to check with whom they do the business. Otherwise, an SSL Certificate doesn't protect such as SQL injections, cross-site scripting or malware.

1.4 Legal obligations

The Dutch Personal Data Protection Act (WBP) requires securing personal data transmission over the Internet. Nevertheless, it happens far too often that this information is sent over the Internet without any means of security.

The consequences for the victims of Internet fraud can be enormous. Criminals intercept personal data, credit card and address information and use these 'stolen identities' for criminal acts like financial transactions. The Dutch government acknowledges the problem. The Dutch Data Protection Authority (CBP) therefore recommends using an SSL Certificate.

SSL Certificate

Personal information is transmitted in several ways; for example, in the case of online purchases and

financial transactions, but also when filling in simple contact forms. In all cases the Dutch DPA requires securing the data. The purchase of an SSL Certificate ensures that the data are safe.

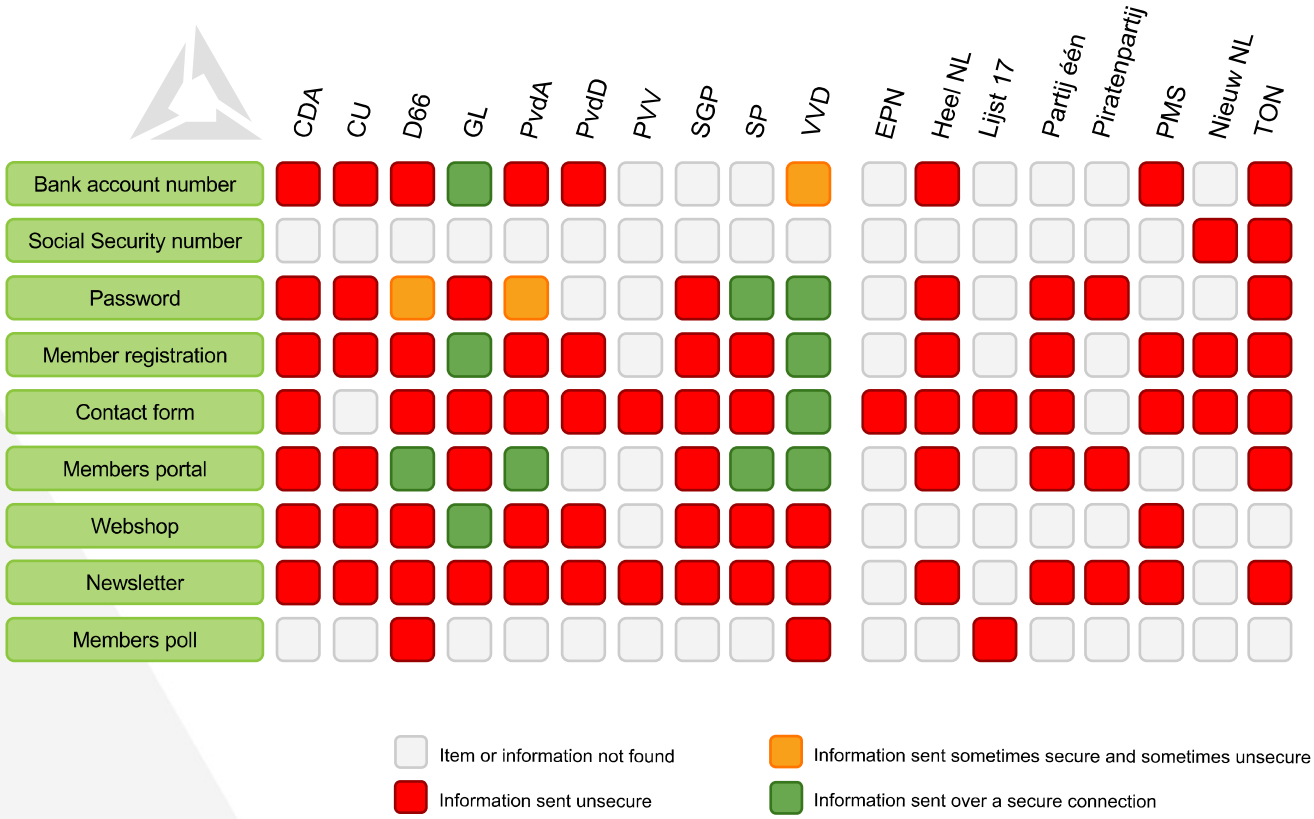
Required

The act requires securing personal data. If you do not comply with the Dutch Personal Data Protection Act, the authorities may impose an administrative fine at a maximum of € 4.500,-. In case one is held responsible for the loss of privacy information or insufficient protection against unauthorized use, full damages and possible claims of individuals involved should be paid for.

2 Featured websites

Networking4all examined the websites of all participating political parties. Here we discuss each site separately and underpin our findings. We also have cited the positions of the parties regarding the protection of personal data and quotes on the websites.

2.1 Crosstab



Explanation crosstab:

The table above shows all investigated parties. Using the colored boxes we indicate whether we have found a section on the site and whether it is safe or not. We have done this to make clear where, how and what information is leaked. In some cases, for a membership a bank account number is requested. Others don't. In this diagram you can see exactly what is sent and is not sent over an insecure connection.

2.2 Per party

Now you will see every political party and what is wrong with their website. Where is that information leaked and what do they say in their statement about online safety and protection of personal data.

2.2.1 CDA

The CDA is very clear about online privacy: “The CDA wants that people get a better grip on their online privacy. The use of privacy-friendly techniques are encouraged. The government should give the right

example for digital developments. Companies must clearly and explicitly ask consumers for permission to collect their online data and linking files (opt-in system).”

The CDA support as government party the expensive campaign in which the citizen is made to be aware of personal data and unsafe websites.

The CDA clearly indicates to stimulate privacy techniques. It is strange the site of the CDA does not have these techniques. The site never protects the personal data of its visitors. Password, bank and address details are sent over an unsecured connection.

2.2.2 ChristenUnie

The party program of the ChristenUnie doesn't say a lot about online safety and protecting individual privacy. It does say this about the Electronic Patient Dossier (EPD): “Ensuring the privacy and confidentiality of data is a requirement for national implementation of EPD.”

Like the CDA and the PvdA, ChristenUnie was the party that has initiated the campaign to raise awareness among the citizens for safety on the web.

It can be concluded that the privacy of citizens is very important. The ChristenUnie seems to consider the danger to its own website smaller. It does not have a secure connection and all data are possible to intercept, including bank details.

2.2.3 D66

“D66 wants to protect privacy on the Internet. Capturing surfing habits, filling out forms etc., should be restricted”, can be found in the D66 party program. Alexander Pechtold also had frequent questions on this topic in the parliament.

You may predict that D66 has her own business in order. This website also don't protects citizens against the interception of information. When someone wants to donate D66 bank details will send over an unsecured connection. A (small) positive point is that log-in information for the intranet of the party are protected. Whether that justifies that D66 is a party which has Web Security top priority, could be the question.

2.2.4 GroenLinks

GroenLinks says in its manifesto that data should be better protected. “Privacy and personal information will be better protected. Digital information systems, services and products are designed that only necessary information is stored for a prescribed purpose and, where possible, anonymous. Citizens and consumers gain insight into the use of their personal data. Without their explicit consent can this information not be sold or shared with third parties.”

Despite the party's affairs in relation to most other parties fairly in order, they are still sending passwords over an unsecured connection. The site has an SSL Certificate, but it is not used at all necessary locations. The personal data are blocked when someone wants to join the party, but not, for example if someone wants to log into the Campaign Center. Personal security appears, certainly in comparison with the other political parties, more important.

2.2.5 PvdA

The site of the PvdA has included a privacy statement which says: “The PvdA is convinced that protecting the privacy of its members and interested visitors to the site is essential for its activities. Personal information of members and interested visitors are secured with the utmost care. The PvdA will comply at all times the requirements of the Personal Data Protection Act” and “if you want to register as a member or for an activity you can sent your personal data and such bank details through a so-called Secure Socket Layer (SSL) connection.”

The research of Networking4all indicates somewhat different. Although the site has an SSL Certificate, the data is not always secure. The text on the website notwithstanding. A certificate is available. The approach of the party is definitely good. The implementation is however not optimal: the certificate is not used everywhere.

As the mayor of Amsterdam Job Cohen improved safety, but he still has a lot to do with website of the PvdA.

2.2.6 Partij voor de Dieren

The Partij voor de Dieren (Party for Animals) believes that “the Personal Data Protection Act should be strengthened to safeguard citizens' rights.”

Maybe the party can better advocate for stricter enforcement of the Personal Data Protection Act. The site does not have an SSL Certificate and sends all data over an unsecured connection. Also in the shop of the party, cybercriminals can intercept data. Without being cynical, the animals may be glad they don't have to fill in their personal data on the website!

2.2.7 PVV

The PVV has nothing in its manifesto about the importance of protecting personal data on the Internet. That's clear when you look on the website. The site has little interaction. Visitors to the site can only use a contact form and subscribe to the newsletter. Over an unsecured connection. So cyber criminals can do a easy job.

What are the consequences if the relevant information can be intercepted by potential Muslim terrorists, Mr. Wilders?

2.2.8 SGP

The Reformed Political Party doesn't say anything about online privacy in its party program. That is evident from the site. It does not have an SSL Certificate and all personal information is sent over an insecure connection. We can conclude that the orthodox party take care with the personal data on an unorthodox way.

2.2.9 SP

It seems protection of personal data is valuable for the SP. They write: “The Data Protection Authority receives more penalty opportunities and should give higher fines when there is violation of privacy.” Internet fraud must also be punished harder, according to the SP. “Police and justice will have greater opportunities to effectively combat for human trafficking, tax evasion and Internet fraud” and “The Internet is a new source of

income for many criminals. They should fight harder against all forms of Internet crime. Illegal gambling via the Internet should be better controlled."

The website of the SP has an SSL Certificate. This is unfortunately not used everywhere. The shop isn't secured and when someone wants to join the party he/she will send the data unsafe. Once a member of the party it is possible to log in on the secure site SPNET. Jan Marijnissen has its heritage rather neatly transferred to Emile Roemer, but also the SP should have a better protected website!

2.2.10 VVD

Some issues on the website of the VVD are secure. It says about the protection of personal data: "Protecting the privacy of citizens is important. Freedom is a great thing. Internet and modern technologies allow to collect large amounts of data, whether it is for fighting terrorism or the patient's file. Too often we have to assume the good intentions of the government, without adequate guarantees and safeguards against abuse. Clear rules about what can and can not and technical safeguards to prevent improper use, are guarantees of freedom for the citizen."

The registration form on website is secure. A normal user can't see this because of the use of an 'invisible' inline frame, which refers to an external secured page. Otherwise, the site of the party itself and the shop are not secured and thus may still be tapped, include bank details.

In short, the website of Mark Rutte isn't really badly, but we doubt if European Commissioner Neelie Kroes of ICT and Telecom can be proud on its website.

2.2.11 Evangelische Partij Nederland

The Evangelical Party of the Netherlands does not focus on data protection in its program. The site does not take measures to protect the personal information that must be managed in the contact form. The site also offers minimal opportunities to interact.

2.2.12 Heel Nederland

Heel Nederland don't discuss the importance of online safety in its manifest. However, it offers its visitors the possibility to become a member and fill in the contact form. Both have an unsecured connection. Again, hackers can so easily tap personal (and bank) details.

2.2.13 Lijst 17

"Private remains private! We soon want to see a dividing line. We actually becoming less secure, despite the motto of security, and our data are more often - sometimes literally – for public use."

That's what 17 Lijst writes about Internet privacy. Personal data are also for public use at Lijst 17. The site does not protect data during transport and visitors who complete the contact form may risk that their completed data are intercepted.

2.2.14 Partij één

Partij één doesn't take any position about online privacy. They don't seems to take the privacy of visitors very seriously. All data must be entered unsecured. The site does therefore not have an SSL Certificate.

2.2.15 Piratenpartij

The main goal of the Piratenpartij is privacy. The first ten pages of the party program are devoted to the importance of privacy. It is regrettable to note that the website itself doesn't deal with privacy that much. Thus, data such as an password will be sent unsecured.

2.2.16 Partij voor Mens en Spirit

“The privacy of ordinary citizens is decreasing, without demonstrable effect on crime and terrorism. Privacy is important because it gives freedom and because hacking and misuse of data are rather simple in this life.”

Similarly to the website of the Party for People and Spirit. The site does not have a secure connection and visitors fill in all data unsecured, including bank details.

2.2.17 Nieuw Nederland

Nieuw Nederland paid no attention to protect personal data on the web in their party program. Is does say on its website that they act in accordance with the Personal Data Protection Act. The test of Networking4all reveals the opposite. Joining the party and filling in the contact form should go through an unsecured connection. Also the Social Security number can be intercepted.

2.2.18 Trots op Nederland

Trots op Nederland has a small note about cybercrime. “The government interferes too much with private affairs and opinions. We make an end to political patronage, even on the internet: no filtering. So the Internet remains free from government influence. Crimes which are crimes in the real world should of course be investigated and prosecuted.”

Trots op Nederland may be more critical on its own website. The site has no protection. Thus, all data (including Social Security numbers and bank details) will send over an insecure connection and malicious could relatively easy intercept this information. The conclusion is justified that we are not really proud of the website of TON!

3 Conclusion

In the Netherlands, the States-General (the lower and upper house) and the government are responsible for legislation in the Netherlands. The Personal Data Protection Act (WBP) may therefore be assumed as known in political parties.

Research of Networking4all shows that only five of the eighteen parties, participating in the parliamentary elections, have taken measures to protect personal data on their website. Unfortunately, the measures taken by these five parties are also inadequate. What is striking is that some parties indeed have an SSL Certificate, but that its not properly applied universally.
Actually we can say that none of the eighteen parties comply with the Personal Data Protection Act.

Which is strange. The parties talk a lot about data protection and privacy regarding the Electronic Patient Record and the Public transport smart card. Last year the topic is frequently put on the political agenda and several Parliamentary questions are made. You would expect that the parties at least protect their own website.

Last year Networking4all point out the government with a report that many government websites leaks data. Measures would be taken as they said. This is what happened in some cases. It is disappointing to notice that the politicians do not even look at their own website.

This study shows that the websites of the eighteen political parties not only sent names and addresses unsecured, but also things like passwords, bank account numbers and social security numbers. Hackers can in many cases relatively easy intercept the information as they are completed on the web.

Of the 'big' parties are mainly the websites of the CDA, SGP, Partij voor de Dieren and the ChristenUnie very bad. At the sites of these parties is nothing blocked and sensitive information is leaked. We definitely expect more of ruling party CDA, which has the Prime Minister as well, who says in its own party program “The government should give the right example in digital developments.”

GroenLinks, SP, VVD, D66 and PvdA seem to have paid most attention to the protection of personal data. Which is striking that the intention of the PvdA looks good, but the implementation isn't. Despite the good intentions, these five parties also don't comply with the Personal Data Protection Act. Montesquieu had certainly expected more from our legislators!

4 Contact

Networking4all B.V.

Postal address:
P.O. Box 15320
1001 MH Amsterdam
Noord-Holland
Nederland

Telephone:
+31 (0)20 - 7881030
Fax:
+31 (0)20 - 7881040

Telephone Belgium:
+32 (0)2 - 8081484

Telephone United Kingdom:
+44 (0)203 - 3184538

Website:
www.networking4all.com

E-mail:
info@networking4all.com

Appointment:

Do you want to see how easy it is to intercept information or making an interview appointment with a specialist of online security? Please contact Paul van Brouwershaven, technical director of Networking4all via +31 (0)20-7881042 or p.vanbrouwershaven@networking4all.com.