AVIS

Avis

Élections pour la Chambre des Députés du 20 octobre 2013

Circonscription électorale SUD

Présentation des listes des candidats :

Le Président du bureau principal de la circonscription électorale Sud (23 députés à élire) recevra les présentations des listes des candidats et les désignations de témoins, en son bureau, au bâtiment de la Justice de Paix à Esch-sur-Alzette, 1er étage, salle d'enquête 4,

le mardi 20 août de 09.00 heures à 12.00 heures,
le mardi 20 août 2013 de 15 heures à 18.00 heures,
le mercredi 21 août 2013 de 09.00 heures à 12 heures et
le mercredi 21 août 2013 de 15 heures à 18 heures.

Le dernier délai utile pour faire les présentations est le mercredi, 21 août 2013 de 17.00 à 18.00 heures. Passé ce délai, aucune présentation de candidats ne sera plus recevable.

Aux fins de la présentation des listes des candidats, des formules imprimées sont mis à la disposition des intéressés à la Justice de Paix à Esch-sur-Alzette, rez-de-chaussée, au guichet.

Esch-sur-Alzette, le 24 juillet 2013
Le juge de paix directeur adjoint
Tom MOES

INSTRUCTIONS AU SUJET DES CANDIDATURES :

Les listes sont constituées pour chaque circonscription par des groupements de candidats qui, par une déclaration signée par eux, acceptent la candidature dans cette circonscription. Les candidats sont présentés conjointement soit par cent électeurs inscrits dans la circonscription, soit par un député élu dans la circonscription, sortant ou en fonction, soit par trois conseillers communaux élus dans une ou plusieurs communes de la circonscription.

Chaque liste doit être déposée par un mandataire désigné par et parmi les présentants de la liste et qui remplit tous les autres devoirs qui lui sont imposés par la loi électorale. En cas de présentation par un député ou par trois conseillers communaux, le mandataire est désigné par les candidats soit parmi les candidats de la liste, soit parmi les élus qui la présentent.

La liste comprend les nom, prénoms, profession et domicile séparément pour les candidats et les présentants.

Un candidat et un présentant ne peuvent figurer que sur une seule liste dans la même circonscription. Nul ne peut être candidat dans plus d'une circonscription.

Une liste ne peut comprendre un nombre de candidats supérieur à celui des députés à élire dans la circonscription.

Toute candidature isolée est considérée comme formant une liste à elle seule.

Chaque liste doit porter une dénomination. Si différentes listes portent des dénominations identiques, les mandataires sont invités à établir les distinctions nécessaires.

Toute liste doit être déposée au plus tard mercredi, le 21 août 2013, avant 18.00 heures.

Lors de la présentation des candidats, le mandataire de la liste peut indiquer, pour assister aux opérations de vote, un témoin et un témoin-suppléant au plus pour chacun des bureaux de vote choisis parmi les électeurs de la commune.

Les mandataires chargés du dépôt des listes sont invités, afin de simplifier les vérifications imposées par la loi, de joindre, tant pour les candidats que pour les présentants, ainsi que pour les témoins, des certificats d'inscription sur la liste électorale, à délivrer par les administrations communales.

DOSSIER INTERNET

MAILDIENSTE

Mitlesen unerwünscht!

Anton Lorenz-Meyer

Maildienste verwerten die persönliche Daten ihrer Nutzer. Es geht aber auch ohne Bespitzelung.

Prism und Tempora - die US-Spähprogramme sind in aller Munde. Der Militärnachrichtendienst NSA hat direkten Zugriff auf die Server von Google, Facebook, Microsoft, Apple und anderen. Was bedeutet, dass über Gmail oder Outlook laufende digitale Kommunikation abgefangen und ausgewertet werden kann.

Die Bespitzelung ist nicht das einzige Ärgernis. Die Firmen, deren Server angezapft werden, scheren sich selbst wenig um die Privatsphäre ihrer Kunden. Google etwa erstellt mit Hilfe von Gmail detaillierte Nutzerprofile und verhökert sie an die Werbeindustrie. Der Nutzer - das wandelnde Datenmateriallager.

Wen interessiert, was da zusammenkommt, der kann „Immersion" herunterladen. Das Massachusetts Institute of Technology hat diese App entwickelt. Der Nutzer erlaubt den Zugriff aufs Konto - und schon wertet das Programm die Metadaten aus: Absender, Empfänger, Datum oder Uhrzeit. Zum Schluss zeigt eine bunte Grafik, was „Immersion" über den Nutzer herausbekommen hat. Dicke Kreise symbolisieren seine häufigsten Kontakte, und Linien stellen Verbindungen zwischen den E-Mail-Empfängern her. Ein ziemlich umfassendes Bild des Privatlebens.

Zum Glück ist der Nutzer nicht dazu verdammt, sich ausspionieren zu lassen. Es gibt alternative Dienste, die darauf verzichten, persönliche Daten auszuschlachten. aikQ ging vor zwei Jahren online. Der Dienst erhebt keine Bestandsdaten. IP-Adressen werden nicht gespeichert, oder genauer, werden in 0.0.0.0. umgeschrieben. Und die Nutzer müssen ihren richtigen Namen nicht angeben. Denn die Anmeldung funktioniert auch mit Pseudonym. Roman Kowalzek: „Wir lassen einfach unnötige Dinge weg."

Für eine sichere Kommunikation ist ebenfalls gesorgt. Die Verbindung vom Nutzer zum Server ist immer verschlüsselt. Auch der Versand der E-Mail erfolgt über verschlüsselte Kommunikationswege. Wobei jedoch zu beachten ist: Verschlüsselt werden nur die Kommunikationskanäle, nicht die Daten selbst .

aikQ unterstützt auch - optional - eine Ende-zu-Ende Verschlüsselung. Hier wird nicht nur die Verbindung, sondern auch die E-Mail verschlüsselt. Der Dienst nutzt dafür den Standard S/Mime. Man bekommt zwei Schlüssel, einen privaten und einen öffentlichen. Die Nutzer - A und B - müssen zuerst ihre öffentlichen Schlüssel austauschen. Danach schreibt A mit dem öffentlichen Schlüssel von B an B. Gelesen werden kann die Nachricht nur von B, weil er allein den privaten Schlüssel besitzt. Eine Einschränkung besteht auch hier: Nur der E-Mail-Text wird verschlüsselt, der Anhang bleibt zugänglich.

Die Passwörter der Nutzer werden in verschlüsselter Form gespeichert, und zwar über einen so genannten Hashwert, eine kryptische Zahlen- und Buchstabenfolge. „Damit der Hashwert noch schwieriger zu lesen

FOTO: UBIQUI / FLICKR

Obamas wahres Gesicht: Der gute demokratische US-Präsident entpuppt sich als Daten-Krake.

ist, salzen wir ihn nochmal mit Zufallszahlen", erklärt Kowalzek. So werde das Ausrechnen des Passworts enorm schwierig.

Jede Verschlüsselung oder Anonymisierung kann geknackt werden.

Ist der E-Mail-Verkehr auch vor Geheimdiensten sicher? Jede Verschlüsselung oder Anonymisierung kann geknackt werden. Will jemand wirklich an die Daten, verschafft er sich früher oder später auch den Zugang. Die Frage ist nur: Wie leicht wird es ihm gemacht? Kowalzek: „Wir erschweren den Zugang auch dadurch, dass wir einfach keine Daten speichern. Wenn jemand abhört, kann er sich nicht einfach aus der Datenbank bedienen. Namen und Adressen muss er schon selber herausfinden."

Für Kowalzek kommt es auch auf den Nutzer an. Er muss vorsichtig mit seinen Daten umgehen. Es gebe eben keine Samariter im Internet. Alle wollen Geld verdienen. Warum frage sich keiner, wie es sein kann, dass Google ein Weltkonzern ist, obwohl da nie ein Cent gezahlt werden muss? Eine Dienstleistung sei eben nie umsonst zu haben. Bezahlt werde immer. Mit den Nutzerdaten als neuer Währung.

Wer seinen digitalen Schriftverkehr über aikQ laufen lassen will, muss dafür zahlen. Ab September kann zwischen den Tarifen Q und Q+ gewählt werden. Sie kosten im Monat 1,00 bzw. 1,50 Euro und haben beide 10 Gigabyte Speicher.

Einem anderen datenschützenden Dienst - Posteo - bescheren die Prism-Enthüllungen derzeit regen Zulauf. „Wir sind um mehr als 30 Prozent gewachsen", sagt Posteo-Mitbegründerin Sabrina Löhr. Die Nutzer kämen von allen großen Anbietern. Es sei eine große Verunsicherung zu spüren.

Posteo will eine Alternative „zu Daten sammelnden Konzernen" sein. Die Anmeldungen erfolgen anonymisiert. Genau wie der Bezahlprozess, der nicht mit den Postfächern verknüpft wird. Posteo speichert keine IP-Adressen beim Besuch der Seite und löscht diese auch aus dem Quelltext der E-Mail. „Wir handeln nach dem Grundsatz der Datensparsamkeit", erklärt Löhr.

Und die Sicherheit? Der Server verschlüsselt die E-Mail-Kommunikation per SSL - allerdings muss der Gegen-Server dies unterstützen. So gesicherte E-Mails kann niemand ohne sehr großen Aufwand zu treiben mitlesen. Auch Adressbuch- und Kalenderdaten können verschlüsselt werden, und zwar mit dem Passwort des Nutzers. Damit ist sogar Posteo, theoretisch, der Zugriff verwehrt. Der Nutzer soll dem Dienst nicht blind vertrauen müssen.

Viele Anfragen, die derzeit eingehen, betreffen Gmail. Der Google-Dienst durchsucht E-Mails automatisiert, um passende Werbung anzuzeigen. Aber Gmail habe auch einen Vorteil, sagt Löhr, es unterstütze als einziger großer Anbieter die verschlüsselte Kommunikation. Was entscheidend ist: Denn es braucht immer zwei Server, um eine sichere Verbindung herzustellen. Eine E-Mail von Posteo zu Gmail wird daher verschlüsselt übertragen - eine E-Mail von Posteo zu einem anderen der großen Anbieter nicht.

Die Verantwortung dürfe nicht auf den Nutzer abgewälzt werden, betont Löhr. Es sei an der Zeit, dass sich auch die Firmen um die Sicherheit der Datenströme kümmern. Sie müssten einfach nur die Verschlüsselung anschalten. Sie sträubten sich aber mit dem Argument, dass dadurch die Kosten immens stiegen. „Wir können das nicht bestätigen", erwidert Löhr.

Posteo-Postfächer kosten einen Euro im Monat. Dafür bekommt der Nutzer zwei Gigabyte Speicher, erweiterbar auf 20. Jedes weitere Gigabyte kostet 0,25 Euro im Monat. „Wir kalkulieren recht knapp", sagt Löhr. Andere Anbieter verlangen oft viel mehr für vergleichbar große Postfächer - bieten aber weniger Datensicherheit und Datenschutz. Posteo hat auch einen ökologischen Anspruch. Es nutze „echten" Ökostrom, nicht den über Zertifikate grün gewaschenen, mit dem viele Rechenzentren oder Webseiten werben. Löhr: „Die Herkunft des Stroms wird in der IT leider viel zu wenig beachtet."

Ende-zu-Ende-Verschlüsselung ist bei Posteo zwar jetzt schon möglich - aber vorerst nur über ein lokales Mailprogramm wie Thunderbird. In Zukunft will der Dienst nicht nur die Verbindung, sondern auch die E-Mail verschlüsseln. Allerdings besteht hierbei ein grundsätzliches Problem: Die zwei bestehenden Standards - Pretty Good Privacy und S/Mime - sind nicht kompatibel. Nur wenn Sender und Empfänger dieselbe Technik nutzen, wird auch verschlüsselt. Edward Snowden, der berühmte „Whistleblower", hält viel von verschlüsselter Kommunikation - kein Wunder, wird er doch von den USA gejagt. In einem Chat mit dem Guardian sagte er, dass Verschlüsselung funktioniere. Starke Kryptografie sei eine der wenigen Dinge, auf die man sich noch verlassen könne.

https://posteo.de/

Startmail heißt das dritte datenschützende Angebot, das in diesem Jahr startet, zuerst als Betaversion. Keine Datenerhebung, keine Nutzerprofile - so lautet das Versprechen der niederländischen Surfboard Holding. Die Firma betreibt schon Startpage, die „diskreteste Suchmaschine der Welt". Jetzt soll die Diskretion auf den E-Mail-Verkehr ausgedehnt werden. Allerdings muss der Nutzer dafür, dass er nicht ausspioniert wird, bezahlen.

GOOGLE GLASSES

Datenbrillen müssen draußen bleiben!

Andreas Lorenz-Meyer

Google hat die ersten Testexemplare seiner Cyberbrille ausgeliefert - für 1.500 US-Dollar das Stück. Allerdings stößt das Gestell auf viel Skepsis ...

Ein Konsument darf mit einem gekauften Produkt machen, was er will? Bei elektronischen Geräten gelten andere Regeln. Ihre Funktionen können zunehmend von außen gesteuert werden. Der Hersteller nimmt sich das Recht der Fernwartung heraus und kann an dem Gerät jederzeit etwas verändern oder sperren. Der Konsument, an der langen Leine gehalten, hat genau genommen nur eine Nutzungslizenz, nicht das Gerät als Ganzes gekauft.

Dass es nur eingeschränkt möglich ist, elektronische Waren wirklich zu besitzen - diese Entwicklung treibt Google auf eine vorläufige Spitze. Die Firma verschickte die ersten Testexemplare seiner Datenbrille - mit strengen Auflagen versehen. Es ist nicht gestattet, die „Explorer Edition" weiterzuverkaufen, zu verleihen oder jemand anderem zu geben, heißt es in den Nutzungsbedingungen.

Google kann leicht überprüfen, ob sich Nutzer daran halten. Sie müssen sich übers Google-Konto registriert haben. Erst dann ist die Datenbrille einsatzbereit. Wird sie an jemand anderen weitergegeben, ist eine Verknüpfung mit dessen Konto notwendig - was Google sofort merken würde.

Die Firma droht mit drakonischen Strafen: Wer die strengen Regeln missachtet, dessen Datenbrille wird deaktiviert - ganz einfach. Ein Amerikaner namens Ed ist schon davor zurückgeschreckt. Er wollte seine Datenbrille auf Ebay versteigern, brach die Auktion dann aber ab. Das bis dahin höchste Gebot hatte immerhin bei über 90.000 US-Dollar gelegen.

Die Brille mit dem kleinen Gehäuse ist begehrt, weil sie neue digitale Erfahrungen möglich macht. Mit Internet und GPS verbunden, kann sie Informationen über die Umgebung ins Gesichtsfeld hineinprojizieren: die Wettervorhersage, Nachrichten, Bahnverbindungen oder der kürzeste Weg zum Museum. Mit dem Gestell lassen sich auch E-Mails schreiben oder Telefonate führen. Der Nutzer muss dabei nichts eintippen, er kann die Befehle über Sprachsteuerung geben. Und um etwas zu hören, ist kein zusätzlicher Kopfhörer nötig. Die Übertragung von Geräuschen erfolgt per Knochenschalltechnik.

Filmen und gefilmt werden

Auf einer Seite des Gestells ist eine Linse montiert, über welche die digitalen Informationen abgebildet werden. Der Bildschirm schwebt also ständig vor dem Auge - was auch gesundheitliche Folgen haben kann, wie Steve Mann vom Massachusetts Institute of Technology im Magazin „IEEE Spectrum" erklärte. Er fürchtet, dass Google unausgereifte Technik anbiete, die der Sehkraft schaden könne. Der Pionier des tragbaren Computers muss es wissen. Schließlich probiert er seine eigenen Modelle selbst aus - und hatte schonmal unter Wahrnehmungsstörungen zu leiden.

Doch bis die Cyberbrillen in der Öffentlichkeit auftauchen, wird es noch ein Weilchen dauern. Vermutlich kommen sie erst nach Weihnachten auf den Massenmarkt, dann für etwa 400 US-Dollar, vermuten die Marktforscher von IHS Insight. Doch schon jetzt erregen sie die Gemüter.

Was nicht an eventuellen Sehstörungen liegt, sondern an der eingebauten Kamera, die Fotos schießt und Videos dreht. Damit kann jeder Passant auf der Straße andere, ohne dass diese es merken, fotografieren oder filmen. Er muss dafür nicht stehen bleiben. Und er muss auch nicht das Smartphone zücken.

Allein das Gefühl, dass andere die Technik missbrauchen könnten, geht auf Kosten der Freiheit, sagen die Kritiker der Datenbrille wie Woodrow Hartzog vom Center for Internet and Society in den USA. Bei „ArsTechnica" sprach der Rechtswissenschaftler von der schlimmsten technologischen Bedrohung der Privatheit im öffentlichen Raum, die er je gesehen habe.

Das Unbehagen, ungewollt aufgenommen zu werden, kann sich überall ausbreiten, nicht nur auf Straßen und Plätzen, auch in geschlossenen Räumen. Der Typ mit der Datenbrille, der mir da gegenübersitzt, hat mich doch nicht etwa gefilmt, als mir eben die Kaffeetasse umgekippt ist? Und das Video dann bei YouTube hochgeladen?

An der Eingangstür von „The 5 Point", einem alteingesessenen Café in Seattle, hängt ein Verbotschild: Auge mit Datenbrille, rot durchgestrichen. Google Glass muss draußen bleiben, lautet die Ansage. Natürlich ist Publicity ein Grund für diese Maßnahme. Dennoch könnten andere - Kinos, Diskotheken, Kneipen, Nachtclubs - dem Beispiel folgen.

Die Datenbrille ist der nächste Schritt ins digitale Zeitalter, früher oder später laufen die Leute mit Computern auf der Nase herum. Mit dem Google-Modell oder einem anderen, zum Beispiel dem zweilinsigen Gestell, das Sony in den Schubladen hat. Fragt sich, welche Regeln und Gesetze diesen technischen Wandel flankieren müssen.

„Stop the Cyborgs" ist eine Initiative von drei Londonern. Sie wollen strenge Regeln für den Gebrauch von Google Glass. Erstens müsse Gesichtserkennung verboten sein. Zweitens solle jeder den Zugriff anderer auf seine persönliche Daten verweigern können, etwa über eine Do not track - Funktion. Drittens hätten gesammelte Daten immer Eigentum des Nutzers zu bleiben. Und viertens sei eine Verschlüsselung notwendig, damit persönliche Daten nicht in die Hände von Sicherheitsdiensten oder der Werbeindustrie gelangen.

Über Google Glass könne eine totale Überwachung unbemerkt durch die Hintertür eintreten, erklären die Londoner auf ihrer Internetseite. Zwar würde schnell Alarm gegeben, wenn Regierungen überall Kameras und Mikrofone aufstellen und die Informationen an eine zentrale Kontrollstelle schicken. Aber ist es denn besser, wenn die Überwachungsgeräte an unseren Köpfen montiert sind?

PROTECTION DES DONNÉES

Un luxe ?

Luc Caregari

Alors que le monde entier commence à se faire à l'idée qu'il faudra mieux protéger ses données, le Luxembourg ne semble pas trop se soucier des nouveaux enjeux. Un retard qui risque de coûter très cher.

Depuis ce jeudi matin, les terminologies « Prism » ou « Tempora » sont devenues un peu plus obsolètes. Car il y a bien pire. Comme vient de le révéler le « whistleblower » - toujours bloqué à l'aéroport de Moscou - Edward Snowden, l'arme ultime de la NSA s'appelle « XKeyscore ». Depuis 2008, ce programme permet aux services de renseignement américains d'accéder à toute information sur le net, sans limitations. De plus, des filtres leurs donnent aussi la possibilité d'encercler des « activités suspectes ». Vous vous trouvez dans un pays arabe et vous communiquez en français ou en allemand ? Bing ! Une petite lampe rouge s'allume dans un bureau secret aux States. Même si le vice-ministre de la justice américain James M. Cole a immédiatement assuré que les services américains n'iraient pas jusqu'à enregistrer des noms, des contenus ou des adresses, la confiance dans de telles allégations est morte depuis longtemps. Au point où même des députés républicains commencent à questionner le bienfondé de tels programmes, même si le gouvernement leur assure qu'il aurait su déjouer des douzaines d'attentats, grâce à l'utilisation de ces métadonnées.

Et que se passe-t-il au Luxembourg au même moment ? Rien, ou pas grand-chose. Avec un ministre de l'économie qui assure aux consommateurs qu'ils pourront de toute façon continuer à télécharger « au noir », un scandale d'espionnage intérieur et politique qui ne scandalise vraiment que ses victimes. Voir aussi la révélation jeudi matin de la radio 100,7 selon laquelle les partis politiques - même déi Lénk - utiliseraient les données personnelles pour mieux cibler leurs électeurs personnels pour leurs campagnes électorales - le pays donne une piètre image de sa conscience des temps qui courent. Surtout s'il essaie de se reconvertir dans le cyberbusiness, une perspective affichée par tous les partis au pouvoir. Mais on peut douter que l'infrastructure en place soit vraiment prête pour une telle évolution. Une anecdote pour preuve : lorsque le ministre des Finances Luc Frieden a présenté il y a deux semaines en grandes pompes le projet « Lux-Ict », ses services avaient tout simplement ommis de réserver l'URL www.luxict.lu à temps. En d'autres mots : le monde de l'internet évolue avec une telle rapidité que le Luxembourg ne peut pas se permettre son retard habituel de cinq à dix ans. C'est « Innovate or Die », comme disait l'ancien ministre de l'économie Jeannot Krecké.

« Innovate or Die »

Pourtant, même au grand-duché il y a des villages gaulois qui tentent d'organiser la résistance en rendant le public conscient des dangers des mondes virtuels. Cela se passe par exemple dans le sous-sol du café Konrad à Luxembourg-Ville, qui, pour mieux rendre l'atmosphère, ressemble à une vraie crypte avec son plafond voûté. Il s'agit de la sixième « Cryptoparty » organisée par le Chaos Computer Club et Hackerspace.lu - deux organisations qui depuis des années représentent la communauté internationale des hackers au Luxembourg. Mais lors du dernier rendez-vous, qui a eu lieu le 25 juillet, les choses étaient un peu différentes. Non pas qu'il y ait eu une affluence de masse dans la cave du café Konrad - on n'en est pas encore là - mais du moins, une équipe de la télé RTL était venue filmer l'événement. La preuve que la cryptographie - donc le fait d'encoder ses données sur internet pour éviter de se faire espionner par qui que ce soit - est en train de devenir de plus en plus populaire au Luxembourg aussi.

Le programme présenté essentiellement lors de cette « Cryptoparty » répond au doux nom de « Tor Project ». Originalement conçu par l'« U.S. Naval Research Laboratory », il est aujourd'hui utilisé par tous ceux qui souhaitent, pour une raison ou pour une autre, encrypter leurs données. Un de leurs principaux représentants n'est autre que Jacob Appelbaum, un « hacker » dont on entend parler de plus en plus dans les médias. En effet, son engagement pour Wikileaks lui a déjà valu des ennuis avec la justice américaine, qui a même obtenu les clés de son compte Twitter.

Comment ça fonctionne ? « Tor Project » est à la base un réseau de tunnels virtuels qui permet aux personnes qui les utilisent de communiquer de façon anonyme. Sur le site www.torproject.org, tout un chacun peut télécharger un programme qui rend anonyme ses connections - que ce soit dans les recherches effectuées sur le net, dans les courriels ou dans les chatrooms. De plus, on peut aussi télécharger sur le site des programmes pour préconfigurer ses clés USB ou CDs afin de les rendre plus sûrs, un programme pour encrypter son smartphone (malheureusement, Orbot ne fonctionne que sur les smartphones configurés sous Android) ou encore un navigateur Tor - qui est amélioré en permanence. Donc, en somme un paquet pour se protéger dans - presque - toutes les situations encourues sur internet. Et gratuit en plus - même si le « Tor Project » vit aussi de donations.

Mais est-ce que cela vous protège vraiment de tomber dans les mailles d'un service secret ? C'était un des points les plus intéressants de la discussion à la dernière « Cryptoparty ». Parce que si vous encryptez vos communications, les services secrets ne peuvent, probablement, pas accéder à vos contenus. Pourtant, ils peuvent savoir que c'est vous qui encryptez vos communications. Ce qui vous rend suspect d'office. Comme quoi, on est encore loin du meilleur des mondes possibles...

La prochaine fois que vous croisez un flyer comme celui-ci, pensez à y aller. Car l'internet, c'est comme le sexe : mieux vaut avoir des rapports protégés.