Die kuberruimte – voordele en nadele*

1. INLEIDING

Daar kan min twyfel bestaan dat die Internet een van die mees impakmakende ontwikkelings is wat ooit deur die mens voortgebring is. Toepassings wat twintig jaar gelede ondenkbaar sou gewees het, is vandag deel van ons daaglikse lewe – voor die hand liggende voorbeelde is byvoorbeeld elektroniese pos, elektroniese handel, sosiale netwerke en baie meer. Vir miljoene mense wat inligting soek, is die Internet die "plek" waar die inligting gekry word – soektogte in fisiese biblioteke is eintlik nie meer nodig nie.

Enige tegnologie het 'n goeie kant, maar normaalweg ook 'n slegte of donker kant – dit geld ook vir die Internet. Die gebruik van die Internet het talle nuwe risiko's geskep, en onverantwoordelike en onnadenkende gebruik van die Internet kan groot probleme skep – vir regerings, maatskappye en ook vir individue.

In komende paragrawe wil ons bietjie dit wat as die Internet bekend staan ondersoek en die voor- en nadele onder die loep neem.

In paragraaf 1 ondersoek ons eers 'n paar definisies om alles in konteks te plaas. Daarna, in paragraaf, 2 bekyk ons 'n paar toepassings wat vandag inherent deel van ons lewens geword het. In paragraaf 3 ondersoek ons die voordele van die Internet, in paragraaf 4 sekere implikasies en in paragraaf 5 nadele en risiko's. Paragraaf 6 beklemtoon die idee van parlementêre oorsig oor Suid-Afrika se kubersekerheid, en in paragraaf 7 is 'n kort opsomming.

2. 'N BIETJIE AGTERGROND

Drie sake veral moet ons bietjie beter definieer. Die drie is die Internet, die Wêreldwye Web en die Kuberruimte.

2.1 Wat is die Internet?

Informeel kan ons die Internet beskryf as 'n globale stelsel van gekoppelde rekenaars en rekenaarnetwerke – dus eintlik 'n netwerk van rekenaarnetwerke. Daar is letterlik miljoene rekenaars en rekenaarnetwerke betrokke, wat behoort aan privaat persone, openbare instansies, maatskappye, regerings, universiteite en ander instansies. In beginsel is elke sodanige rekenaar eintlik aan elke ander een verbind, en data en inligting kan tussen die rekenaars uitgeruil word.

Niemand weet presies wat die grense van die Internet is nie, en basies is dit nie moontlik om dit te bepaal nie omdat daar daagliks talle rekenaars en netwerke bygevoeg en ook verwyder word. Die Internet word eintlik ook nie deur 'n spesifieke persoon of instansie beheer of bestuur nie.

2.2 Wat is die Wêreldwye Web (WWW)?

Informeel kan ons die WWW beskou as die stelsel van die miljoene der miljoene dokumente wat op die rekenaars van die Internet gestoor en via die Internet bygekom en herwin kan word. Ons

* Voordrag gelewer tydens die simposium van die Suid-Afrikaanse Akademie vir Wetenskap en Kuns te Pretoria in Junie 2012.

kan dus basies die WWW beskou as ’n stelsel wat die Internet as onderliggende infrastruktuur gebruik om gebergde dokumente te vind en te gebruik.

Met behulp van ’n sogenaamde webleser (“browser”) kan ’n persoon nou vanaf sy eie rekenaar ’n spesifieke dokument wat iewers deel is van die WWW vind en aflaai na sy eie rekenaar. Die Internet is dus die struktuur wat dit moontlik maak om by dokumente wat in die WWW gestoor is, uit te kom.

Dit is onmoontlik om die grootte van, dit wil sê die aantal dokumente in, die WWW te bepaal, maar skattings van tientalle biljoene is nie onrealisties nie.

2.3 Wat is die kuberruimte?

Weereens kan ons die begrip van die kuberruimte op verskillende maniere definieer, maar basies kan ons sê dat die kuberruimte ’n tipe samevoeging van die Internet en die WWW is. Dit is die elektroniese ruimte wat bestaan as gevolg van die Internet en die WWW.

Wanneer mens ’n dokument probeer vind in die WWW, dan is jy eintlik besig om in die kuberruimte rond te swerf. As jy ’n e-posboodskap vir iemand stuur, beweeg die boodskap via die kuberruimte van jou af na die ontvanger.

Met die bietjie agtergrond, kan ons nou kyk na die voordele van die kuberruimte.

3. VOORDELE VAN DIE KUBERRUIMTE

Soos hierbo gestel, stel die kuberruimte (die Internet en die WWW) ons in staat om dinge te doen wat twintig jaar terug ondenkbaar (en basies onmoontlik) was. Laat ons ’n paar ondersoek.

3.1 **E-pos** – die stuur van elektroniese boodskappe aan mense wat dwarsoor die wêreld versprei is, sonder om eers presies te weet waar die ontvanger op daardie stadium is, is al algemene gebruik – dit alles binne sekondes.

3.2 **Soekenjins** – die vind van inligting oor omtrent enige onderwerp onder die son binne sekondes.

3.3 **Elektroniese handel** – die uitvoer van ’n wye verskeidenheid elektroniese handeltransaksies, byvoorbeeld elektroniese plekbespreking in hotelle en op vliegtuie, die bestel en koop van ’n elektroniese boek, die betaling daarvan en die onmiddellike aflaai daarvan op jou rekenaar of elektroniese leser en elektroniese bankwese waar mens al jou finansiële transaksies kan doen sonder om ooit eers in ’n fisiese bank te kom.

3.4 **Elektroniese kontak met regeringstelsels** – die elektroniese hantering van jou inkomste-belasting, aansoeke by regeringsdepartemente en ander.

3.5 **Sosiale netwerke** – die uitruil van inligting tussen vriende.

In Suid-Afrika alleen word geskat dat 150 000 klein en medium grootte maatskappye bestaan en opereer as gevolg van hulle kuberteenwoordigheid en dat meer as 1,5 miljoen werksgeleenthede in sulke klein maatskappye deur dié teenwoordigheid onderhou word.

Bogenoemde is maar ’n klein deeltjie van wat elke dag in die kuberruimte plaasvind. Soos die Internet en WWW ontwikkel in die volgende paar jaar, sal daar nuwe toevoegings wees wat ons lewens nog meer gaan beïnvloed.

Voordat ons die negatiewe kant van die kuberruimte bekyk, laat ons net kortliks sekere implikasies ondersoek wat vloei uit die voordele wat hierbo bespreek is.

4. IMPLIKASIES

Die groter gebruik van die kuberruimte vir toepassings soos hierbo genoem, en veel meer, het uiteraard sekere implikasies vir die gebruikers daarvan.

Die eerste belangrikste gevolge is dat gebruikers meer en meer persoonlike inligting in die kuberruimte stoor. As mens byvoorbeeld via die WWW vir een of ander kompetisie inskryf, word heelwat inligting gevra wat dan in die betrokke maatskappy se databasisse gestoor word. As mens 'n plekbespreking deur die WWW doen, gebeur presies dieselfde. Op dié manier word ons persoonlike inligting geleidelik op talle plekke in die kuberruimte gestoor, en ons is nie eers altyd bewus daarvan nie. Sosiale netwerke soos Facebook is ook 'n goeie voorbeeld. Miljoene mense se persoonlike inligting, sommige baie persoonlik, word iewers in die kuberruimte gestoor, en dis amper onmoontlik om dit weer te vind en uit te wis.

Voorts is dit algemene gebruik dat maatskappye wat sulke databasisse het oor gebruikers, kliënte ensovoorts, dit weer verkoop aan ander mense wat weer beteken dat die persoonlike inligting nog eens op nog plekke gestoor word.

As die inligting net vir wettige en gemagtigde redes gebruik word, sal dit seker in orde wees, maar die WWW se data is ook die teiken van mense wat die inligting wil bekom en op ongemagtigde maniere wil gebruik, wat lei tot kubermisdaad. Statistieke toon dat kubermisdaad tans die omvattendste vorm van misdaad in die wêreld is, en ander tipes misdaad soos dwelmmisdaad en onwettige wapenhandel verby gesteek het. Daar word beweer dat Suid-Afrika tans ongeveer R 1 biljoen rand per jaar verloor weens kubermisdaad.

Dat die Internet en WWW ongekende voordele vir die mens inhou, is 'n feit, maar soos hierbo bespreek, het die saak ook 'n negatiewe kant. Laat ons daardie kant 'n bietjie bekyk.

5. NADELE/RISIKO'S VAN DIE KUBERRUIMTE

Laat ons die risiko's op drie vlakke bespreek, naamlik die risiko op persoonlike vlak, op besigheidsvlak en op regeringsvlak.

5.1 Risiko's op persoonlike vlak

Die belangrikste risiko op hierdie vlak is elektroniese identiteitsdiefstal.

5.1.1 Wat is elektroniese identiteitsdiefstal?

Die persoonlike gebruiker van die kuberruimte is voortdurend die teiken van kubermisdadigers. Die hoofdoel van aanvalle is identiteitsdiefstal. Laat ons die begrip identeitsdiefstal vereenvoudig deur te sê dis die diefstal van jou aantekenkodes (wagwoorde) tot 'n stelsel, byvoorbeeld tot jou elektroniese bankstelsel, jou sosiale netwerkstelsel, jou e-posstelsel en ander. As die kubermisdadiger die kodes kan bekom, dan kan hy jou identeit aanneem en inteken op die stelsel – die stelsel sal dit aanvaar want 'n rekenaarstelsel kontroleer net of die betrokke kodes korrek is – die stelsel het geen idee wie dit invoer nie. Nou kan die kubermisdadiger in jou bankstelsel inkom en jou geld steel deur dit oor te plaas na 'n nuutgeskepte rekening, hy kan op jou sosiale netwerkprofiel aanteken en enige ongure en onwaar inligting die kuberruimte instuur en almal sal dink dit kom van jou af, hy kan op jou e-posstelsel inteken, en jou e-pos lees of vals

e-posboodskappe in jou naam stuur en so meer. Ander onaangename gevolge kan byvoorbeeld kuberagtervolging wees ("cyber stalking") waar die misdadiger jou persoonlike inligting soos huistelefoonnommer en fisiese adres bekom, en jou dan op allerhande maniere terroriseer.

Kuberboeliery ("cyber bullying") is ook 'n misdaad wat onrusbarend toeneem. Veral onder kinders vind kuberboeliery plaas deur die gebruik van selfone.

Die verlies van jou elektroniese identiteit veroorsaak ongelooflike probleme vir mense op alle gebiede en is nie iets wat maklik ongedaan gemaak kan word nie. Enige gebruiker van die kuberruimte moet dus bewus wees van die tegnieke wat gebruik word om jou identiteit te steel, en watter beskermingsmaatreëls getref moet word om dit te bekamp.

5.1.2 Watter tegnieke word gebruik vir identiteitsdiefstal?

Hoewel daar talle tegnieke is, moet ons konsentreer op drie hoofkategorieë naamlik sosiale manipulering ("social engineering"), kwaadwillige programmatuur en die uitbuiting van bedryfstelselkwesbaarhede.

5.1.2.1 Sosiale manipuleringstegnieke

Hier probeer die misdadiger jou aantekenkodes in die hande kry deur veral internethengel ("phishing").

Die tegniek behels dat die gebruiker 'n e-posboodskap kry wat oënskynlik van die bank af kom of van die e-posadministrasie afdeling. Daarin word die gebruiker meegedeel dat daar een of ander probleem met sy rekening is, en dat hy net vinnig moet aanteken om seker te maak dat alles nog reg is. 'n WWW-skakel word dan verskaf waarop die gebruiker moet klik. Indien hy dit doen, word hy gekoppel aan 'n webbladsy wat presies lyk soos die een waaraan hy gewoond is. Hierdie is egter 'n herleide webbladsy ("spoofed page") wat eintlik aan die misdadiger behoort. Indien die gebruiker nou wel aanteken op die bladsy, wat hy dink sy bank se bladsy is, maak hy egter 'n reuse fout want die misdadiger kry onmiddellik die aantekenkodes, teken dan dadelik aan op die bank se korrekte webbladsy met die gesteelde aantekenkodes en voer ongemagtigde transaksies uit.

5.1.2.2 Kwaadwillige programmatuur ("malicious software/malware")

Wanneer 'n mens inligting op die WWW soek, en iets kry waarna jy gesoek het, word die inligting afgelaai na jou eie rekenaar toe. Jy het dus toegang gekry tot die betrokke webwerf, maar die webwerf het ook toegang tot jou rekenaar nodig om die gevraagde inligting af te laai na jou rekenaar. 'n Mens vertrou altyd dat die inligting wat afgelaai word presies is wat jy gevra het, en nie ander ongevraagde inhoud ook bevat nie. Dit is egter presies hier waar die kubermisdadiger misbruik maak van die algemene vertroue van WWW-gebruikers.

Statistieke bewys dat talle webwerwe geïnfekteer is met kwaadwillige programmatuur wat dan onwetend op jou rekenaar afgelaai word. Sodanige kwaadwillige programmatuur het verskillende name, byvoorbeeld virusse, Trojaanse perde, wurms en ander. Die kwaadwillige programmatuur kan allerhande dinge doen, maar een van die gevaarlikstes, en mees gebruiktes, is om byvoorbeeld sogenaamde sleutelbordkopieerderprogrammatuur op jou rekenaar af te laai. Elke sleutel wat jy daarna op jou rekenaar druk, word dan deur die sleutelbordkopieerderprogrammatuur onderskep en teruggestuur na die misdadiger wat die stukkie programmatuur geskep het. Op dié manier kan die misdadiger jou elektroniese bankstelsel se kodes onderskep wanneer jy

weer heel onskuldig aanteken na jou bankstelsel, en onmiddellik is jou elektroniese identiteit (en jou geld) gesteel!

Jou rekenaar kan ook geïnfekteer word deur die kwaadwillige programmatuur in te bed in een of ander aanhangsel wat aan 'n e-posboodskap geheg word. Die gebruiker word dan gevra om die aanhangsel oop te maak deur daarop te klik. Die oomblik as dit gebeur, word jou rekenaar geïnfekteer deur die kwaadwillige programmatuur wat in die aanhangsel versteek was, met dieselfde gevolge as hierbo genoem.

Ander ongemagtigde aksies kan wees om jou data te kopieer en terug te stuur aan die misdadiger, om jou data te vernietig, om die e-posadresse op jou adreslys te steel en baie ander skrikwekkende dinge.

5.1.2.3 Die uitbuiting van bedryfstelselkwesbaarhede

Die bedryfstelsel van 'n rekenaar, byvoorbeeld Windows, bestaan uit miljoene lyne programmeringskode en dit is onmoontlik om dit behoorlik en volledig te toets. Dus word daar gedurig kwesbaarhede (foute) ontdek. In baie gevalle skep sulke kwesbaarhede die geleentheid om die bedryfstelsel te infekteer met kwaadwillige programmatuur, en dan is ons terug by die vorige paragraaf. Dieselfde aspek geld ook vir die webleser, byvoorbeeld Internet Explorer, wat gebruik mag word.

Enige gebruiker moet deurentyd bedag wees op die aanvalstegnieke wat hierbo bespreek is, en voorsorgmaatreëls daarteen tref. Laat ons kortliks kyk wat is die noodsaaklike voorsorgmaatreëls teen die drie tegnieke wat hierbo genoem is.

5.1.3 Wat kan mens doen om die risiko's te verminder?

5.1.3.1 Teen sosiale manipulering

Die belangrikste voorsorgmaatreël hier is om niemand te vertrou nie.

Moenie reageer op e-posboodskappe wat jou vra om enige aantekeninligting op enige manier te verskaf nie – dit is 'n vorm van 'n kuberaanval op jou.

Moenie reageer op enige e-posboodskap wat beweer jy het geld of enigiets anders gewen nie – dis 'n vorm van 'n aanval op jou want hulle soek jou bankbesonderhede (om uiteindelik jou geld te steel).

5.1.3.2 Teen kwaadwillige programmatuur

Sorg dat jy 'n goeie anti-virusprogram geïnstalleer het. So 'n program behoort talle stukke kwaadwillige programmatuur te herken en toegang tot jou rekenaar te weier.

Sorg dat jou anti-virusprogrammatuur op datum bly. Nuwe stukke kwaadwillige programmatuur verskyn daagliks, en as jou anti-virusprogrammatuur nie bygewerk is nie, gaan dit nie die nuwes herken en keer nie.

Probeer 'n persoonlike brandmuur ("firewall") installeer wat ook sal help om jou rekenaar beter te beveilig.

Moet nooit aanhangsels tot e-posboodskappe oopmaak as jy nie doodseker is van wie dit kom nie.

Die ontstellende situasie is egter dat die nuutste kwaadwillige programmatuur so gesofistikeerd is dat selfs die nuutste en mees bygewerkte antiviruspakkette nie in staat is om sulke kwaadwillige programmatuur te herken of op te spoor nie!

5.1.3.3 Teen uitbuiting van bedryfstelselkwesbaarhede

Sorg dat jy gereeld die kwesbaarheidsopdatering van die maatskappy wat jou bedryfstelsel of webleser ontwikkel het, op jou rekenaar aanbring om die geïdentifiseerde kwesbaarhede toe te stop. As jy dit nie doen nie, bly jou rekenaar kwesbaar.

5.1.3.4 Algemene opmerkings en advies

Moet nie naïef wees en die kuberruimte vertrou nie – dis die wilde weste daarbuite!

Moet nie persoonlike inligting verskaf as dit nie werklik nodig is nie – dink baie mooi voor jy dit doen

As jy 'n Facebookprofiel het, stoor die minimum persoonlike data daarop want dit kan gesteel word en teen jou gebruik word

Moenie dink jy is anoniem as jy in die kuberruimte rondswerf nie – verskeie komponente van jou elektroniese identiteit word op tallose plekke op die WWW vasgelê tydens elke swerftog

Wees versigtig – wees baie versigtig!

5.2 Risiko's op maatskappyvlak

Internasionale statistieke bewys dat veral klein en medium grootte maatskappye wat die WWW gebruik vir besigheidsdoeleindes, al meer die teiken word van kubermisdadigers. Sulke maatskappye bevat dikwels sensitiewe inligting soos kliëntkredietkaartnommers, wat die eerste prys vir sulke misdadigers is.

Weens 'n beperkte ruimte kan daar nie op hierdie aspek uitgebrei word nie, maar maatskappye moet sorg dat hulle inligting- en kubersekerheid behoorlik op datum is. Talle gevalle is gedokumenteer waar kubermisdadigers kredietkaartinligting uit maatskappye se databasisse gesteel het en dit op die WWW gepubliseer of ongemagtig gebruik het. In baie gevalle het sulke maatskappye se reputasie ongelooflik skade gely.

5.3 Risiko's op regeringsvlak

Regerings, en ook die Suid-Afrikaanse Regering, het groot rekenaarstelsels met massiewe databasisse wat sensitiewe en persoonlike inligting bevat. In baie gevalle laat hulle gebruikers toe om toegang tot die stelsels te kry via die Internet. Voorbeelde is die stelsels van die Ontvanger, die Departement van Binnelandse Sake en ander. Inligting- en kubersekerheid is dus ook van die hoogste prioriteit in al die gevalle.

6. PARLEMENTÊRE OORSIG OOR KUBERSEKERHEID IN SUID-AFRIKA

Op dié stadium behoort dit duidelik te wees dat kubermisdaad 'n baie groot probleem is en dat gewone gebruikers totaal uitgelewer is aan die gesofistikeerde tegnieke van die kubermisdadigers. Voorts word persoonlike inligting in talle maatskappy- en Regeringsdatabasisse gestoor, waarvan baie potensieel deur kubermisdadigers bygekom kan word – dis die ekwivalent van 'n reuse kuberaanval op inligting. As landsburgers het ons die reg om te weet hoe goed ons persoonlike inligting in sulke databasisse beskerm word. Ongelukkig is daar tans geen manier waarop ons antwoorde op vrae soos die volgende kan kry nie :

Wie verseker dat my persoonlike inligting in privaat- en regeringsdatabasisse behoorlik beskerm is?

Wie roep maatskappye en regeringsdepartemente tot verantwoording wanneer inligting gekompromitteer word?

Waar gaan kla die gewone burger as hy die slagoffer van kubermisdaad geword het?

Die skrywer huldig die opinie dat Suid-Afrika dringend 'n nasionale Parlementêre Staande Komitee oor Kubersekerheid nodig het om Internet- en WWW-gebruikers in Suid-Afrika te help beskerm. So 'n komitee moet ook help verseker dat alle instansies wat sensitiewe inligting in hulle rekenaarstelsels stoor en wat 'n kuberteenwoordigheid het, behoorlike inligting- en kubersekerheid implementeer.

7. OPSOMMING

Die Internet, WWW en kuberruimte het ongelooflike voordele, maar as dit nie behoorlik bestuur en beskerm word nie, ly almal daaronder.

Prof Basie von Solms
Direkteur: Sentrum vir Kubersekerheid, Universiteit van Johannesburg
basievs@uj.ac.za