Nieuwsbrief 4-2012

W.Bosgra ***Taakaccenthouder digitale criminaliteit***

Digitale nieuwsbrief samengesteld door Secure Computing.

Doel is bewustwording van wat u doet met de computer en kennis opdoen voor de opsporing van strafbare feiten gepleegd middels de computer. U kunt deze nieuwsbrief opslaan op uw eigen "Home"-omgeving en als naslagwerk blijven gebruiken.

Deze nieuwsbrief zal met enige regelmaat in uw mailbox verschijnen.

Middels deze nieuwsbrief houden wij u op de hoogte van:

- onderwerpen die betrekking hebben op het veilig gebruik van de computer en het internet
- nieuws uit de media
- juridische vragen
- nieuwe technieken
- vele andere wetenswaardigheden

In deze editie o.a

E-mail spoofing

Veilig internetbankieren? Gebruik een live cd/dvd!

Cloudcomputing

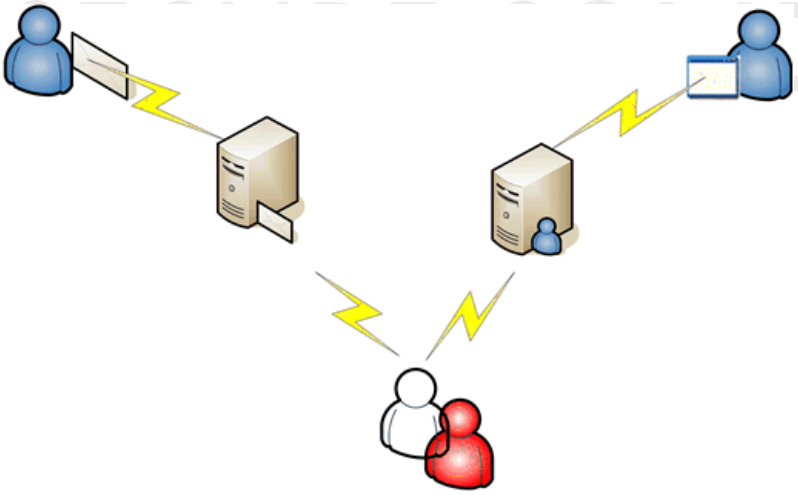
E-mail spoofing:

“Mijn e-mail account is gehackt. Mensen ontvangen e-mail van mij, welke ik niet heb opgesteld en heb verstuurd”.

Vervolgens wordt een aangifte opgenomen ter zake Computervredebreuk. U herkent dit vast wel. Echter hoeft er geen sprake te zijn van Computervredebreuk. Een nieuw fenomeen wat de kop opsteekt is E-mail spoofing.

E-mail spoofing is een term die gebruikt wordt om frauduleuze e-mailactiviteiten te beschrijven. Deze activiteiten houden in dat specifieke eigenschappen van het e-mail bericht, zoals From (Van), Return-Path (Afzender) en Reply-To (Antwoorden naar) worden gewijzigd, waardoor het lijkt dat de e-mail bij een andere bron vandaan komt. E-mail spoofing is een veelgebruikte techniek voor het versturen van spam.

Ook zijn er computervirussen welke e-mail spoofing gebruiken om zichzelf te verspreiden. Het virus gebruikt een ander adres dat het op de geïnfecteerde computer heeft aangetroffen als afzender. In sommige gevallen maakt het virus ook zelf een e-mailadres aan. Mensen van wie de computer geïnfecteerd is, kunnen moeilijk worden gewaarschuwd, omdat hun e-mailadres voor de meeste ontvangers onbekend is.



Wie maakt er gebruik van e-mailspoofing en waarom? E-mailspoofing wordt voornamelijk gebruikt om twee redenen:

Om een onbestaand afzendadres mee te geven. In veel gevallen van spam wordt gebruik gemaakt van een onbestaand afzendadres. De afzender van de spam heeft dus niet alleen een ander adres meegegeven als afzendadres, maar zelfs een adres dat helemaal niet bestaat. De reden hiervoor is dat spammers vaak absoluut niet geïnteresseerd zijn in antwoorden per e-mail, maar zoveel mogelijk mensen willen leiden naar hun website waarop zij hun producten aanbieden.

Om een bestaand adres van een ander mee te geven. Het meegeven van een bestaand adres van een ander heeft natuurlijk als voornaamste doel de ontvanger te laten denken dat de e-mail ECHT van die ander vandaan komt. Dit kan autoriteit uitstralen of vertrouwen inboezemen. Er zijn twee vaak voorkomende gevallen waarbij een bestaand adres van een ander wordt gebruikt:

Virussen die zichzelf via e-mail versturen geven er de voorkeur aan om bestaande e-mailadressen als afzendadres te gebruiken. Sommige virussen gebruiken telkens hetzelfde adres (bijvoorbeeld een virus dat zichzelf als Microsoft verzendt), sommige virussen maken met behulp van informatie van de geïnfecteerde computer een afzendadres (bijvoorbeeld) en weer andere virussen zoeken op de

geïnfecteerde computer naar adressen en gebruiken die. Het doel is hier om vertrouwen in te boezemen. Als u erin trapt en denkt dat de e-mail echt bij Microsoft vandaan komt, dan is de kans groter dat u de e-mail en eventuele bijlage opent. De kans dat het virus zichzelf verder kan verspreiden wordt op die manier dus groter.

phishers gebruiken e-mailadressen van de organisaties die ze imiteren, met als doel autoriteit en vertrouwen uit te stralen. Als een phisher uw creditcardgegevens wil achterhalen dan is het van belang dat u gelooft dat de e-mail ook echt van uw creditcardverstrekker vandaan komt.

Kortom: e-mailspoofing wordt op grote schaal gebruikt door virussen, spammers en phishers, met als doel om vertrouwen en autoriteit uit te stralen.

Hoe herken je e-mailspoofing en wat kun je ertegen doen?

Als individuele gebruiker kunt u weinig doen tegen e-mailspoofing. Als u een e-mail heeft ontvangen dan heeft het feitelijke spoofen al plaatsgevonden. In deze gevallen is het belangrijk dat u gespoofde e-mail kunt herkennen. E-mailspoofing is in sommige gevallen te ontdekken door naar de zogenaamde headers te kijken van de e-mail (zie nieuwsbrief 1-2012).

Hoe herken je een daadwerkelijk gehackt e-mailaccount.

1. vraag of er e-mail berichten zijn verwijderd

2. staan er te verzenden e-mail berichten klaar die geweigerd zijn door ontvangers?

3. men kan niet meer met het eigen wachtwoord inloggen

4. persoonlijke instellingen zijn veranderd

Indien hier sprake van is heeft men daadwerkelijk het e-mail account gehackt.

Elekronisch briefgeheim?

Het briefgeheim geldt niet voor e-mail. Internetproviders hebben wel een geheimhoudingsplicht voor mail van en naar hun klanten. En de schrijver van een e-mail kan via zijn auteursrecht optreden tegen ongewenste publicatie.

Voor papieren post bestaat sinds de negentiende eeuw het grondwettelijk briefgeheim. Dit betekent dat de overheid niet zomaar de post van haar burgers mag inzien of onderscheppen. Alleen op grond van wettelijke uitzonderingen (bijvoorbeeld een huiszoekingsbevel of een sterk vermoeden dat er een bom in de brief zit) mag een bepaalde brief worden geopend door een opsporingsdienst.

Tegenwoordig wordt er steeds meer met elektronische post (e-mail) gecommuniceerd. Het briefgeheim voor papieren post is geregeld in de Grondwet. Dit geldt niet voor e-mail. Voor het afluisteren van elektronische communicatie zijn wel aparte regels in het Wetboek van Strafrecht opgenomen, als onderdeel van de wetten over computercriminaliteit.

Afgeven van klantgegevens

Om iemand aansprakelijk te stellen voor onrechtmatig gedrag op internet, zijn adresgegevens nodig. In de meeste gevallen heeft alleen zijn provider die gegevens. Op grond van jurisprudentie zijn providers verplicht deze NAW-gegevens af te geven als de eiser daar een redelijk belang bij heeft.

Een provider is dan misschien niet aansprakelijk voor onrechtmatige informatie die zijn klanten aanbieden, die klant is dat natuurlijk wel. Maar om die juridisch aansprakelijk te kunnen stellen, moet je wel weten waar hij woont. In de meeste gevallen heb je als klager niet meer dan een IP-adres of een e-mailadres. Dat is niet genoeg om een dagvaarding uit te kunnen brengen.

De provider van de persoon die dat IP-adres of mailadres gebruikte, weet dat wel. Providers houden bij wie van hun klanten welk IP-adres gebruikt op welk tijdstip. En mailproviders (zoals Hotmail) registreren van elke uitgaande mail welk IP-adres gebruikt werd bij het aanmaken of versturen. Vandaar de trend om providers een kort geding aan te doen om op basis van IP-adres of email de persoonsgegevens van hun klanten te krijgen, wanneer die klanten iets onrechtmatigs gedaan hebben.

Een provider kan verplicht worden door de rechter om persoonsgegevens af te geven. Daarbij geldt een vierstappentoets, zoals geformuleerd door de Hoge Raad.

1. de mogelijkheid dat de informatie, op zichzelf beschouwd, jegens de derde onrechtmatig en schadelijk is, is voldoende aannemelijk;
2. de derde heeft een reëel belang bij de verkrijging van de NAW-gegevens;
3. aannemelijk is dat er in het concrete geval geen minder ingrijpende mogelijkheid bestaat om de NAW-gegevens te achterhalen;
4. afweging van de betrokken belangen van de derde, de serviceprovider en de websitehouder (voor zover kenbaar) brengt mee dat het belang van de derde behoort te prevaleren.

In een situatie waarin aan al deze eisen is voldaan, is het volgens de HR redelijk om te eisen dat de provider de adresgegevens van de klant afgeeft.

Veilig internet bankieren? Gebruik een live CD/DVD.

Een steeds groter aantal mensen wordt slachtoffer van fraude tijdens het internetbankieren. Op de computer geplaatste virussen, trojaanse paarden en keyloggers, stelen uw inloggegevens en vervolgens worden geldbedragen van uw rekening overgeboekt naar exotische oorden. Dit kun je voorkomen door een zogenaamde live cd/dvd te gebruiken voor het internetbankieren c.q het gebruik van het internet.

Een Live CD/DVD is een besturingssysteem opgeslagen op een zelfstartende cd-rom/dvd. Het besturingssysteem kan worden gebruikt zonder installatie op een harde schijf. Na uitname van de cd-rom/dvd kan de computer weer normaal starten met het op de harde schijf aanwezige besturingssysteem. Een Live cd/dvd heeft als basis het Linux besturingssysteem.

Voordeel is dat er dus geen gebruik wordt gemaakt van bestanden aanwezig op uw computer. Hierdoor hebben virussen , trojaanse paarden en keyloggers geen kans.

Welke Livecd/dvd kan ik gebruiken?

Omdat de meeste mensen een Windows besturingssysteem gebruiken ben ik op zoek gegaan naar een Live cd/dvd, die wat betreft layout en gebruik het meest overeen komt met Windows. Ik adviseer derhalve het gebruik van een Zorin OS Live cd/dvd. Zorin OS is gebaseerd op de Ubuntu linux distributie, bekend van de IRN internetpc's.

Zorin OS is echter gebruiksvriendelijker . Momenteel is Zorin OS 5.2 de laatste versie.

Downloaden kunt u hier: www.zorin-os.com/free.html

Als alternatief kunt u Ubuntu 11.10 proberen.
http://www.ubuntu.com/download/ubuntu/download

Na het downloaden heeft u een zogenaamd imagebestand op uw pc. Deze dient op een dvd gebrand te worden. U kunt hiervoor het gratis programma ImgBurn gebruiken. (www.imgburn.com/index.php?act=download)

Na het branden beschikt u over een Live cd/dvd waarmee u de computer kunt opstarten.

Gebruik:

Eerste voorwaarde is, dat het opstartmenu van uw computer, uw dvdspeler als eerste opstarmedium heeft staan in het bootmenu in de BIOS van de computer. Dit hoeft u slechts eenmalig aan te passen. U komt in de BIOS van uw computer door tijdens het opstarten op Delete, F2 of F8 te drukken (dit kan per computer verschillen). Als het BIOS verschijnt gaat u naar het tab blad waaronder de opstartvolgorde (bootmenu) staat aangegeven. Bekijk de aanwijzingen om de volgorde te wijzigen. Zet uw cd/dvd drive op plaats 1. Daarna opslaan en afsluiten. De computer start nu opnieuw op. Vervolgens plaatst u de live cd/dvd in uw dvdspeler en start opnieuw op. Nu wordt tijdens het opstarten de gegevens op de live cd/dvd ingelezen. Als dit klaar is ziet u een menu. Kies hier **niet** voor installeren, maar voor live gebruiken. Wacht dan tot uiteindelijk het besturingssysteem klaar is voor gebruik.

Een Live CD start iedere keer op dezelfde manier. Het starten duurt wat langer, omdat alle aanwezige hardware afgezocht en ingesteld moet worden. Omdat een cd-rom langzamer is dan een harde schijf, is het werken met een Live CD wat langzamer.

Daarnaast kan het starten van programma's langer duren, omdat deze meestal gecomprimeerd op de schijf staan.

Na gebruik van de live cd/dvd sluit u af, neemt de cd/dvd uit uw computer en herstart deze. U hoeft geen veranderingen in het BIOS aan te brengen. Als er geen disk in de dvdspeler zit, start Windows normaal op. Plaatst u de volgende keer opnieuw de live cd/dvd als u deze weer wilt gebruiken en herstart uw computer.

Overigens kunt u een livecd/dvd ook voor andere toepassingen gebruiken. Een Live CD heeft verder de volgende toepassingen:

- De meest gebruikte toepassing is om kennis te maken met een ander besturingssysteem, zonder dat het eerst geïnstalleerd hoeft te worden.
- Een Live CD/dvd kan gebruikt worden ter controle van de computer. Doordat er niets op de harde schijf wordt geschreven, kunnen veilig de gegevens op de computer bekeken worden.
- Wanneer een computer vanwege technische of softwaregebreken niet meer goed van de harde schijf start (of zelfs helemaal niet meer wil starten), biedt de Live CD vaak uitkomst op twee manieren:
- Enerzijds kan men gewoon verder werken (onafhankelijk van de harde schijf); Anderzijds kan men softwareproblemen op de harde schijf oplossen of belangrijke bestanden vanaf de harde schijf op bijvoorbeeld een USB-stick veiligstellen. De Live CD als probleemoplosser wordt ook wel "rescue cd" genoemd.

LET OP: ook het gebruik van een Live cd/dvd helpt niet om te voorkomen dat u slachtoffer wordt van Phishing (nagemaakte website). Klik derhalve ook bij gebruik van een Live cd/dvd nooit op een hyperlink – bijv. in een email of via een andere website - om bij uw bankwebsite te komen. **Type deze altijd handmatig in**! Doe dit uiteraard ook als u Windows gebruikt.

Het advies om een opstartbare Live CD/DVD te gebruiken zegt niet: Gebruik Linux ipv Windows. Ook Linux is vatbaar voor keyloggers als je het installeert op je computer. Gebruik van een Live CD/DVD om te booten – op te starten- en dan het internet op te gaan, is dus een stuk slimmer.

Cloudcomputing

Cloud computing is de nieuwe trend op internetgebied. Het lijkt een hype, maar net als bij voorganger 'Web 2.0' is vooralsnog onduidelijk wat de term precies inhoudt.

Als introductie is het goed te weten dat Engelstaligen met 'the cloud' meestal gewoon 'het internet' bedoelen. Het is de 'wolk' waarin alles gebeurt. Een vrij recente ontwikkeling is echter dat internet niet alleen een publicatiemiddel is (voor software, in dit geval), maar dat daadwerkelijk rekenkracht op afstand wordt gebruikt. Helemaal nieuw zijn alle concepten niet, maar het totaalbeeld dat ontstaat dwingt tot een nieuwe manier van denken over het gebruik van de computercapaciteit die op het internet is aangesloten.

IT'ers gebruiken de term 'cloud computing' op verschillende manieren. Zo zijn er techneuten die het zien als een soort uitbreiding van het begrip server, terwijl anderen bepleiten dat eigenlijk alles wat buiten de eigen firewall draait al 'in the cloud' is.

Cloud computing betekent dus verschillende dingen voor verschillende groepen mensen.

Wie vandaag googelt naar cloud, komt wellicht niet langer eerst bij de weerman terecht. Internetbedrijven die onlinediensten aanbieden maken met deze term het mooie weer, en de kans is groot dat ook jij al stevig actief bent in die cloud.

Gebruik je Gmail of Live Hotmail? Heb je al een document bewerkt met behulp van Google Docs of Office Web Apps? Het zit allemaal in de cloud. Veel heeft dus met internet te maken, en niet toevallig wordt dat sinds jaar en dag als een wolk afgebeeld.

Waarom zou je?

Het grootste voordeel is dat je de dienst, net als de data, van overal kunt benaderen. Of toch zolang je over een (fatsoenlijke) internetverbinding beschikt. Dat kan vanaf je pc of Mac zijn, maar net zo goed vanaf je laptop, je smartphone of zelfs je spelconsole.

Ook niet onaardig: je beschikt automatisch over de recentste versie van de cloudapplicatie, tenminste als die geen desktoppoot heeft (lees: een programma dat je eerst moet installeren).

Nadelen zijn er uiteraard ook. Vooral als er veel uploads mee gemoeid zijn kan een verblijf in de cloud je wel eens zuur opbreken. Privacy is een ander heikel punt, want je mag niet vergeten dat je (soms erg persoonlijke of delicate) data in handen van een derde partij geeft.

Ben je zeker dat die gegevens onderweg niet gekaapt kunnen worden? Met andere woorden: dat ze versleuteld worden verstuurd én dat ze op de servers zelf geëncrypteerd worden opgeslagen? Vooral aanbieders van gratis cloudapplicaties geven amper garanties op het vlak van uptime en werking. Server gecrasht? Vergeet het maar dat je aan je data kan. Provider failliet? Dan ook!

Hou er bovendien rekening mee dat je gegevens, zonder dat je het goed beseft, vaak op een buitenlandse server terechtkomen – niet zelden van een Amerikaans bedrijf, waar de overheid maar met de Patriot Act hoeft te zwaaien om inzage te vorderen.

Opslag

Online opslag is wellicht de populairste dienst in de cloud, vooral voor het maken van back-ups. Dat hoeft niet echt te verbazen. Meestal komen je gegevens in professionele datacenters terecht en worden er automatisch spiegelkopieën gemaakt. In elk geval worden je bestanden off-site bewaard

en in tegenstelling tot back-ups op een externe schijf, blijven je data intact wanneer je het slachtoffer wordt van een virus, brand of diefstal.

Wil je gegevens in the cloud gaan opslaan, kijk dan eens naar het gratis Microsoft SkyDrive. Gratis 25 gigabyte opslagruimte en vanaf elke computer te benaderen, waar ter wereld je ook bent.

Hoe veilig is mijn cloud?

Alles wat u aan een webdienst toevertrouwt, is potentieel in gevaar. Laten we eerlijk zijn: het staat op internet, u hebt nauwelijks controle over het beveiligingsbeleid van de dienst, en u staat met lege handen als de cloud door een storing alles kwijtraakt. Als de door u gebruikte dienst gehackt wordt, hebben criminelen toegang tot alles wat u daar bewaart. De beveiliging is net zo sterk als de zwakste schakel. Kies in ieder geval altijd een ijzersterk cryptisch wachtwoord voor de diensten die u afneemt op internet, en gebruik nooit en te nimmer hetzelfde wachtwoord voor een andere dienst.
Tegenover deze schaduwzijden staat dat cloud-diensten zeer veel gebruiksgemak en flexibiliteit opleveren. Door zelf een back-upplan te maken voor de cloud-diensten waarvan u het meest afhankelijk bent - bijvoorbeeld uw Gmail, Office Live Workspace-documenten en de lopende projecten in uw Dropbox -, bent u in ieder geval goed gewapend tegen een crash van de cloud of andere vorm van gegevensverlies.

Wat kan IK verder “in the cloud”?

Googel maar eens op de termen Online Tool / Online Programs en je zult zien dat er voor bijna elke applicatie die niet op uw computer is geïnstalleerd, er een online versie voor te vinden is. Het voordeel hiervan is dat je dus programma’s kunt gebruiken die niet op je computer geïnstalleerd staan. Denk bijvoorbeeld aan fotobewerking, bestandsconversie enz.

Een paar voorbeelden >

Online presentatie maken:

ZOHO Show beta

https://show.zoho.com/login.do

Online tekstverwerker:

ZOHO Writer beta

https://writer.zoho.com/jsp/home.jsp

Bestanden omzetten:

ZAMZAR™ Free online file conversion

http://www.zamzar.com/

Online tekst vertalen:

YAHOO! BABEL FISH

http://babelfish.yahoo.com/

en voor nog veel meer programma’s:

GO2WEB20 .net WEB APPLICATIONS INDEX

http://www.go2web20.net/