INTERNET SCHOON

Wat kun je doen om jouw steentje bij te dragen?

"Samen sterker voor waarborging van een veilig, vrij en open internet"

bit
internet technology

Geen gewoon internet, maar Internet Schoon

Internet en IT zijn van groot maatschappelijk belang en hebben een positief effect op de Nederlandse economie. Op het moment dat de IT-markt groeit, wordt echter ook de afhankelijkheid groter. Denk alleen al aan de gevolgen van de continue stroom aan cyberincidenten, waarmee bedrijven het risico lopen compleet platgelegd te worden. Bovendien neemt ook de druk op het milieu toe.

Om ervoor te zorgen dat we maximaal blijven profiteren van de voordelen van IT, is het tijd dat we als IT-professionals allemaal ons steentje bijdragen aan een schoon internet. Dit vraagt om concrete acties op het gebied van privacy, security en duurzaamheid.

Natuurlijk is onlangs de AVG van kracht geworden, maar dit is slechts een eerste stap richting een duurzaam privacy- en securitybeleid. Een veilig en schoon internet moet de standaard zijn voor iedere IT-afdeling. Daarom roepen wij je op om jouw verantwoordelijkheid te pakken om er samen voor te zorgen dat Nederland vandaag en in de toekomst zorgeloos kan profiteren van alle digitale mogelijkheden.

Om je op weg te helpen in de strijd naar een schoon internet, hebben wij dit e-book opgesteld. Aan de hand van de drie Internet Schoon-aspecten, privacy, security en duurzaamheid, hebben we een aantal praktische handvatten opgesteld. Dit zijn suggesties om je op weg te helpen. Kies maatregelen die bij jouw organisatie passen en pas deze dan stap voor stap toe. Zo staan we samen sterker in de strijd voor een veilig, vrij en open internet met waarborging van privacy.

PRIVACY **SECURITY** **DUURZAAMHEID**

"Een veilig en schoon internet moet de standaard zijn voor iedere IT-afdeling"

bit internet technology

Inhoudsopgave

bit internet technology

1. Privacy: zorgeloos internet

Nog te vaak horen we ondernemers roepen 'Ik maak geen gebruik van persoonsgegevens'. Hier gaan je haren van overeind staan, want iedere organisatie beschikt bijvoorbeeld al over een salarisadministratie en dus persoonsgegevens. Maar denk ook aan de database vol gegevens van relaties, zoals klanten en leveranciers. Het is zaak om stil te staan bij de hoeveelheid persoonsgegevens waarover de organisatie beschikt en de manier van verwerking. Wanneer verwerk je welke persoonsgegevens? Heb je alle gegevens wel echt nodig? En hoe kunnen we ervoor zorgen dat het internet weer betrouwbaar wordt? Om dit zo goed mogelijk in te regelen, behandelt dit hoofdstuk met name de privacy-by-design en privacy-by-default-principes. Privacy is een cruciaal onderdeel van Internet Schoon. Niet alleen vanuit principiële en ethische overwegingen, maar zeker ook ter bescherming van jouw medewerkers, (potentiële) klanten en organisatie.

"Privacy is een cruciaal onderdeel van Internet Schoon"

1.1 Privacy-by-design

Privacy-by-design houdt in dat vanaf de start van de ontwikkeling van informatiesystemen rekening wordt gehouden met privacy. Een mooie manier om de beveiliging van persoonsgegevens te optimaliseren, omdat er direct vanaf het ontwerp al aandacht voor is. Dit betekent echter niet dat je alleen aan het begin aandacht aan privacy besteedt. Gedurende de totale levensduur van het systeem moet je na blijven denken over de noodzaak van het opslaan van gegevens en de levenscyclus van de data. Hoe ga je om met het opslaan, wijzigen en verwijderen van data?

Dataminimalisatie

Begin met het toepassen van dataminimalisatie. Verzamel geen overbodige gegevens en ga na welke gegevens je daadwerkelijk nodig hebt om jouw dienst of product te kunnen leveren. Denk bijvoorbeeld aan een contactformulier op de website. Vraag je ook naar het privéadres? Vraag jezelf dan af of dit wel echt noodzakelijk is. Ga je de persoon in kwestie ook per post benaderen? Data die je niet verzamelt, hoef je ook niet te beveiligen. Het scheelt je tijd en de data loopt geen onnodig risico.

Pseudonimiseren

Heb je bepaalde gegevens toch nodig? Dan is het belangrijk om deze zo snel mogelijk te pseudonimiseren. Zorg dat identificerende gegevens zoals naam, IP-adres en Burgerservicenummer vervangen worden door een code, indien deze data niet in zijn originele vorm wordt gebruikt – zoals in verreweg de meeste gevallen geldt. Hierdoor is de betrokkene niet meer identificeerbaar, maar nog wel individualiseerbaar. Hierbij is het belangrijk dat gegevens versleuteld worden opgeslagen door middel van encryptie, zodat deze alleen beschikbaar zijn voor verwerkingsbevoegden.

Bewaren en verwijderen van data

Tot slot zitten aan het bewaren van persoonsgegevens ook regels verbonden. Persoonsgegevens worden met een bepaald doel verzameld en verwerkt. Het bewaren is dan ook slechts toegestaan voor zover dit noodzakelijk is voor het verwerkelijken van dit doel. Dit is een algemene regel waarvan de uitwerking per situatie kan verschillen. Is het doel waarvoor de persoonsgegevens zijn verwerkt niet meer aanwezig, dan dienen deze te worden verwijderd. Om het verwijderen van data soepel te laten verlopen, is het goed om systemen in te bouwen die ervoor zorgen dat gegevens automatisch worden verwijderd.

De AVG-privacyrechten

Onder de AVG (Algemene Verordering Gegevensbescherming) zijn een aantal privacyrechten uitgebreid en zijn er twee nieuwe rechten toegevoegd.

De nieuwe rechten:

- ***Het recht op dataportabiliteit:*** dit is een nieuw recht, om persoonsgegevens over te dragen. Om hieraan te voldoen is het belangrijk om na te denken over hoe de data snel en eenvoudig overdraagbaar wordt. Data moet worden versleuteld, maar dus ook weer ontsleuteld, zodat anderen de gegevens in een format ontvangen waarmee zij aan de slag kunnen. Daarnaast heeft de betrokkene het recht om de persoonsgegevens over te dragen aan een andere aanbieder. En ook hierbij geldt dat de data direct werkbaar is voor de nieuwe aanbieder.
- ***Het recht op vergetelheid:*** dit is een nieuw recht om 'vergeten te worden'. Dit betekent dat alle aanwezige persoonsgegevens uit de systemen verwijderd dienen te worden. Hierbij is het belangrijk om na te gaan dat de data daadwerkelijk overal gewist wordt. Er zijn mogelijk kopieën vanuit de database gemaakt en daarnaast dienen de gegevens ook uit back-ups gewist te worden.

De uitgebreide rechten:

- ***Het recht op inzage:*** het recht van mensen om de persoonsgegevens die een organisatie van hen verwerkt in te zien.
- ***Het recht op rectificatie en aanvulling:*** het recht om de persoonsgegevens die een organisatie verwerkt te wijzigen.
- ***Het recht op beperking van de verwerking:*** het recht om minder gegevens te laten verwerken.
- ***Het recht met betrekking tot geautomatiseerde besluitvorming en profilering:*** het recht op een menselijke blik bij besluiten.
- ***Het recht om bezwaar te maken tegen de gegevensbewerking.***

Het risico van tracking

Overal waar Google Analytics of bijvoorbeeld een Facebook tracking pixel wordt gebruikt, worden bezoekers gevolgd. Veel organisaties maken gebruik van trackingsoftware die de website-ontwikkelaar heeft geïmplementeerd. Website-eigenaren zijn zich hier niet altijd van bewust, maar verzamelen zo wel bezoekersgegevens en vaak zonder bedrijfseconomische redenen.

Tools als Google Analytics lijken wellicht onschuldig, maar ongemerkt komen alle gegevens van jouw websitebezoekers bij Google terecht. Omdat analysediensten gecentraliseerd zijn bij grote partijen hebben zij oneindig veel informatie over gebruikers. Hiermee maakt de betreffende organisatie een zeer gedetailleerd profiel van iedere unieke bezoeker, ingelogd of niet. Wanneer een gebruiker ingelogd is bij Google of Facebook kan er gemakkelijk een profiel worden opgesteld. Zo niet, wordt er een profiel gemaakt op basis van kenmerken zoals IP-adres en/of browserfingerprint.

Het is van belang dat je in kaart brengt welke informatie jouw bedrijf verzamelt en vervolgens kritisch kijkt of deze data daadwerkelijk nodig is. Zo bescherm je de privacy van jouw websitebezoekers optimaal.

"Bescherm de privacy van je websitebezoekers"

1.2 Privacy-by-default

Privacy-by-default wordt vaak in een adem genoemd met privacy-by-design, maar er is een verschil. Privacy-by-default betreft de standaardinstellingen van een programma, app, website of dienst, die de privacy maximaal waarborgt. Daarnaast moeten de algemene voorwaarden ook privacyvriendelijk zijn, wat betekent dat je richtlijnen of statements met betrekking tot privacy niet verstopt. Denk bijvoorbeeld aan een applicatie met 'Privacy' als menu-item, maar daarnaast een item 'Advertenties' waar het delen van gegevens met derden wordt genoemd. Dit moet op één duidelijke plek inzichtelijk zijn. Tevens moet gewerkt worden met opt-ins in plaats van opt-outs; pas als iemand zich ergens voor aanmeldt ontvangt hij informatie.

Veel websites en met name sociale netwerken willen zo veel mogelijk informatie verkrijgen over hun gebruikers. Deze kennis en inzichten worden bijvoorbeeld ingezet bij het uitbreiden van het dienstaanbod. Ook wordt informatie doorverkocht, zodat er relevantere advertenties worden getoond voor de betreffende gebruiker. De standaardinstellingen dienen zodanig te zijn dat deze garant staan voor maximale privacy, omdat gebruikers vaak deze instellingen kiezen of accepteren – als gevolg van gebrek aan kennis of uit gemak.

"Nee hoor, uw data verlaat het pand niet"

"Onlangs ging ik langs de notaris om een juridische overeenkomst voor een stichting te ondertekenen. Hiervoor is natuurlijk ook een kopie van het paspoort nodig en deze had ik zelf meegenomen. Echter wilde de notaris deze kopieën zelf maken, waarop ik vroeg wat hij eigenlijk met het paspoort gaat doen. Het antwoord was dat het niets bijzonders was, maar puur voor de administratie. Bovendien zouden de documenten het pand niet verlaten. Terwijl de secretaresse de kopieën maakte, kreeg de notaris een telefoontje. Toen de documenten weer voor mij lagen, heb ik hier even in gekeken. Het zijn tenslotte mijn eigen persoonsgegevens. Tot mijn verbazing zag ik dat het paspoort door een online dienst was gecontroleerd op diefstal."

Wido Potters,
Manager Support & Sales bij BIT

1.3 Privacy dreigt voor de happy few te worden

Privacy is een grondrecht dat nu belangrijker is dan ooit. Helaas wordt privacy alleen maar duurder. Gratis diensten zijn immers niet gratis, deze worden afgerekend met privacygegevens. Denk maar eens aan zorgverzekeraars die korting bieden in ruil voor data of supermarkten met hun klantenkaarten. Zo'n kaart geeft weliswaar korting, maar verzamelt ook voortdurend gegevens waarmee de koper wordt geprofileerd op basis van het koopgedrag. Oftewel, je betaalt meer als je jouw privacy wilt behouden. En dit gebeurt ook aan de lopende band in de digitale wereld. Gratis diensten van bijvoorbeeld Google en Facebook verzamelen continu gegevens van bezoekers en verkopen deze door aan derden. Dat we toch massaal gebruikmaken van deze diensten heeft twee voorname redenen, namelijk kosten en gemak. Dit is zorgwekkend, zeker als we nagaan dat niet iedereen de mogelijkheid heeft om voor de duurdere optie te gaan. Privacy wordt dan iets voor de elite. Dat creëert een tweedeling in de maatschappij waar we ons tegen moeten verzetten. Bedenk daarom van tevoren waar een gratis dienst zijn omzet vandaan haalt en maak een bewuste keuze in de diensten die je afneemt. Overweeg bijvoorbeeld om zelf een mailserver te hosten als alternatief voor een gratis maildienst.

Waarborg privacy van bezoekers met alternatieve tools

Gegevens verzamelen, maar toch privacy waarborgen? Daar bestaan alternatieve tools voor! Een voorbeeld hiervan is Matomo (voorheen Piwik). Deze open-source software kun je zelf installeren op jouw webhostingpakket. Door middel van een trackingcode op de website verzamelt de tool gegevens zoals de duur van het websitebezoek, de schermresolutie en het land waar je bezoeker zich bevindt. Er wordt een profiel gemaakt van iedere bezoeker, maar deze wordt wel geanonimiseerd. Op die manier heb je inzichtelijk welke pagina's goed scoren, waar de interesses van de bezoekers liggen en welke pagina's onder handen moeten worden genomen. Een ander voorbeeld is LimeSurvey, in plaats van SurveyMonkey – waarbij je respondenten naar een unieke URL linkt om vragen te beantwoorden en gegevens achter te laten, welke vervolgens door derden ingezet kunnen worden bij bijvoorbeeld targeting. LimeSurvey draait daarentegen op een eigen infrastructuur. Een derde voorbeeld is MailChimp, waarin je jouw hele nieuwsbriefdatabase uploadt en klikgedrag wordt bijgehouden. Waarom zou je nieuwsbrieven niet vanuit je eigen mailserver versturen? In het kader van privacyborging de betere oplossing.

2. Security: veilig internet

Dagelijks worden we doodgegooid met krantenkoppen over cybercrime. Hierbij gaat het over externe bedreigingen zoals gestolen data, hacks, DDoS-aanvallen op banken en ga zo maar door, maar ook over interne bedreigingen, zoals een verloren usb-stick of het openen van een schadelijke link. We kunnen dus niet meer zonder security-oplossingen en -maatregelen. Helaas vallen nog teveel organisaties ten prooi aan cybercriminelen. Veelal ligt de oorzaak in het gebrek aan securitybeleid, patches en gebrek aan aandacht voor en kennis over security. Om een veilig internet te waarborgen, vinden wij security dan ook een essentieel onderdeel van Internet Schoon. In dit hoofdstuk vind je enkele (van de talloze) handvatten die je op weg helpen. Het is geen uitputtende lijst.

"We kunnen niet meer zonder security-oplossingen en -maatregelen"

2.1 Informatiebeveiliging: wat moet je doen voordat het misgaat

Privacy en security zijn geen bijzaken, maar randvoorwaarden om een veilig, vrij en open internet te waarborgen. Daarom is het essentieel om in ieder geval een vijftal zaken op het gebied van informatiebeveiliging al in te regelen voordat het misgaat. Zo voorkom je een hoop stress en ellende en hoef je niet langer meer brandjes te blussen.

Verantwoordelijke informatiebeveiliging

Security is niet voor eenieder de core business. We begrijpen dan ook heel goed dat het een lastige klus kan zijn, maar thuis draai je ook de deuren op slot. Wanneer je iemand aanstelt als verantwoordelijke voor informatiebeveiliging, wordt het al iets gemakkelijker. Deze persoon kan de aandacht specifiek richten op het veiligstellen van jouw data. Op deze manier hoeven er achteraf, als het eigenlijk al te laat is, geen maatregelen meer genomen te worden.

Maak een risicoanalyse

Het doel van een risicoanalyse is te bepalen welke bedreigingen de grootste risico's vormen. Er worden vragen beantwoord zoals: Welke bedreigingen zijn er? Wat is de kans dat deze werkelijkheid worden? Wat is de impact? Welke maatregelen hebben we al genomen en welke kunnen we nog nemen? Wanneer de risico's de acceptatiedrempel overschrijden, kan er een verbeterprocedure gestart worden. Op die manier wordt de kans of de impact van de bedreiging gereduceerd en kan tijdig worden ingegrepen. Dit is wel afhankelijk van zaken als techniek en financiën.

Door bijvoorbeeld een Business Impact Analyse (BIA) uit te voeren, krijg je inzicht in de risico's voor jouw organisatie. Met dit inzicht kun je mogelijke schade, bijvoorbeeld financieel of aan het imago, voorkomen. Het is daarom zaak om inzichtelijk te maken welke informatiesystemen jouw organisatie gebruikt en deze te classificeren. Dit kan door middel van de BIV-classificatie; BIV staat voor beschikbaarheid, integriteit en vertrouwelijkheid. Door informatiesystemen te beoordelen op deze drie punten kun je gericht maatregelen treffen. Als beschikbaarheid het belangrijkste punt is dan is het draaiende houden van de server van groot belang. Het is dan aan te raden het systeem redundant uit te voeren. Is integriteit hoofdzaak dan is correctheid van gegevens cruciaal. Een passende maatregel is het read-only beschikbaar maken van data en het toepassen van versiebeheer inclusief logging hiervan. Als vertrouwelijkheid bovenaan staat moet er gewaarborgd worden dat gegevens niet in verkeerde handen vallen. Om dit te realiseren biedt role based toegang tot data, firewalls en access lists uitkomst.

Niet alle informatie is even vertrouwelijk of hoeft bij een incident even snel weer beschikbaar te zijn. Het is niet erg efficiënt of gebruiksvriendelijk om niet-vertrouwelijke informatie op dezelfde manier te beschermen als vertrouwelijke informatie. Bovendien kan de waarde van informatie in de loop van de tijd veranderen, bijvoorbeeld door veranderende processen. Ook het niveau van dreiging kan veranderen en daardoor dus ook de benodigde beschermingsmaatregelen.

Stel een calamiteitenplan op

Een calamiteitenplan is er in alle vormen en maten. Middels dit plan kan er invulling worden gegeven aan issuemanagement, gebouwontruiming, omgaan met milieurampen, en noem maar op. De doelstelling is om de vitale bedrijfsprocessen te continueren in een calamiteitensituatie. Om dat te bereiken moeten er een aantal zaken in kaart worden gebracht. Denk hierbij aan wie welke taak heeft, contactgegevens van medewerkers, autoriteiten en klanten, welke procedures en werkinstructies gevolgd moeten worden bij calamiteiten en een communicatiebeleid.

Er moet bekend zijn welke processen essentieel zijn voor de bedrijfsvoering. Dit lijkt wellicht voor de hand liggend, maar in veel gevallen wordt deze stap overgeslagen. Men denkt toch meer aan technologische oplossingen dan het geautomatiseerd inregelen van back-ups of vanuit de calamiteit zelf. Het is beter om dit om te draaien, dus niet de calamiteit maar de bedrijfsprocessen leidend maken.

Creëer een recoveryplan

Organisaties zijn in groeiende mate afhankelijk van IT-systemen voor bedrijfskritische activiteiten en diensten. Hierdoor heeft de beschikbaarheid van deze systemen een grote impact op de bedrijfsvoering. Het is zaak dat deze beschermd worden, maar deze blijken nog veelvuldig kwetsbaar voor calamiteiten. Het kan gaan over ‘grote’ calamiteiten, zoals brand of wateroverlast, maar ook om ‘kleine’ calamiteiten, zoals een virus of een serverstoring. In een recoveryplan wordt beschreven welke aanpak gehanteerd wordt in zo’n situatie.

Responsible disclosure beleid

Floor Terra, een software developer die zich hard maakt voor een veilige digitale wereld, is de grondlegger van de responsible disclosure. Hackers die gedreven door nieuwsgierigheid lekken in systemen en software vinden, bevinden zich vaak in een juridisch grijs gebied. Ook al hebben ze geen kwade bedoelingen, vaak is het voor hen niet aantrekkelijk om een organisatie te informeren over de lek. Het komt namelijk veel voor dat organisaties niets met de melding doen, slecht communiceren met de melder of zelfs ontkennen dat er een probleem is. Het kan zelfs voorkomen dat een melder te maken krijgt met strafrechtelijke gevolgen. Het is dan ook begrijpelijk dat veel hackers niet de moeite nemen om lekken te melden. Wanneer bedrijven nadenken over hoe ze omgaan met beveiligings-lekken en dit duidelijk naar buiten communiceren, weten hackers waar ze aan toe zijn. Dit voorkomt onzekerheid en paniek aan beide kanten en beperkt schade zoveel mogelijk. (Responsibledisclosure.nl, 2018) De afspraken tussen de organisatie en de melder worden opgesteld en openbaar gemaakt in een responsible disclosure beleid. Hierin staan het verhelpen van kwetsbaarheden en het verhogen van de veiligheid van informatiesystemen centraal. Het is dus een perfect onderdeel om het internet schoon te maken.

Responsible disclosure template

Hoe je dit beleid opstelt, kun je terugvinden in het responsible disclosure template dat is opgesteld door Floor Terra. Dit template beschrijft het beleid van het fictieve bedrijf ACME corporation als aanvulling op de leidraad responsible disclosure die het NCSC heeft gepubliceerd. Baken hierbij goed af wat acceptabele aanvalsmethoden en doelen zijn. De voorbeelden in het template kunnen in principe door alle organisaties toegepast worden.

2.2 Security-by-design

Net als privacy-by-design is het principe van security-by-design om al tijdens het ontwerp van een nieuwe applicatie of het inrichten van een IT-omgeving rekening te houden met de beveiliging. Securityfouten worden met deze werkwijze effectiever verwijderd, doordat je niet wacht op de testfase en fouten direct ondervangt. Zo anticipeer je op risico's en maak je security een integraal onderdeel van iedere oplossing.

Denk ook bij het implementeren en in gebruik nemen van nieuwe informatiesystemen aan de autorisatie van rechten. Welke gebruiker heeft toegang tot welke systemen en bestanden? Bedenk hierbij goed wat een gebruiker daadwerkelijk nodig heeft, zodat onbevoegden geen toegang tot gevoelige informatie en systemen hebben.

"Maak van je security een integraal onderdeel van iedere oplossing!"

2.3 Back-ups voorkomen onnodig dataverlies

Dat een goede back-up belangrijk is staat als een paal boven water. We weten het allemaal, maar in de praktijk gaat het toch nog vaak mis. Dit hangt vaak samen met het feit dat er geen beleid is. Het is daarom belangrijk dat de IT-afdeling hierin proactief haar rol pakt en een beleid opstelt. Dit begint met inzicht in wie welke informatie gebruikt, wie er verantwoordelijk voor is en waar de informatie is opgeslagen. Naast het inregelen van back-ups is ook restoren van groot belang; hierdoor weet je pas echt of de back-up zijn vruchten afwerpt. Een periodieke restoretest verzekert je van een back-up die volledig is. Een goede manier om back-ups te beveiligen is encryptie – de back-up wordt versleuteld, waardoor het risico dat data in verkeerde handen terechtkomt wordt geminimaliseerd.

2.4 Automatiseer patches

Het uitvoeren van een patchbeleid zou eigenlijk de standaard moeten zijn, maar toch gebeurt het lang niet overal. Het gaat hierbij om de installatie van patches op devices, operating systems en applicaties. De urgentie voor het uitvoeren van de patches wordt vaak onderschat, terwijl dit grote privacy- en securityproblemen voorkomt. Geef daarom in een beleid richting aan het patchproces en toets stelselmatig of securitypatches worden opgevolgd en zo niet wat daar dan de reden voor is. Stel bij voorkeur in dat patches automatisch geüpdatet worden, dan weet je zeker dat het gebeurt.

2.5 Werkbare wachtwoordpolicies

Op het moment dat een e-mailaccount wordt gehackt, is het geen grote stap meer om ook toegang te krijgen tot andere online accounts en wellicht bedrijfssystemen. Het enige dat nu nog hoeft te gebeuren is op andere sites aangeven dat het wachtwoord vergeten is en de toegang tot een volgend account is ook geregeld. Voor je er erg in hebt, beschikt een cybercrimineel over toegang tot belangrijke data van jouw organisatie.

Hoe ga je hier slim mee om? Want over het algemeen ervaren we wachtwoorden als lastig en vervelend. Het feit is wel dat ze onmisbaar zijn en we er dus mee om moeten leren gaan. Een zwak of ontbrekend wachtwoordbeleid is een risico waaraan organisaties zichzelf en hun medewerkers blootstellen. Op het moment dat werknemers de vrijheid krijgen, gaat het mis. Aan de andere kant moeten we ook niet doorslaan door het afdwingen van unieke wachtwoorden met minimaal 25 tekens, die ook nog eens maandelijks veranderd moeten worden. Er moet een balans zijn, maar het moet wel afgedwongen en gecontroleerd kunnen worden. Wachtwoordpolicies moeten dus strikt, maar werkbaar zijn, zodat mensen er niet omheen gaan werken. Stel daarom passwordgenerators en passwordmanagers beschikbaar, zodat het voor medewerkers eenvoudiger wordt om voor iedere dienst een uniek wachtwoord te hanteren.

Tot slot is het raadzaam om vanuit de IT-afdeling maatregelen als single-sign-on en two-factor authentication te hanteren. Dit voorkomt een hoop ellende met wachtwoordonveiligheid.

'Have I been pwned?'
"haveibeenpwned.com is ontwikkeld om iedereen snel te laten beoordelen of ze mogelijk in gevaar zijn gebracht door een online account waarin ze zijn gehackt of 'pwned' zijn in een datalek. De site is opgezet nadat er bij Adobe inloggegevens van gebruikers waren gelekt. Je kunt als individu gebruikmaken van deze dienst, maar het mooie is dat je ook als beheerder van een domein kunt aangeven dat je geïnformeerd wilt worden als er een wachtwoord uit jouw domein gelekt is."

Alex Bik, CTO bij BIT

2.7 Toepassen van internetstandaarden

Dankzij de hedendaagse internetstandaarden wordt cybercriminaliteit al voor een deel ingeperkt. Er zijn zonder veel kosten of moeite goede functionaliteiten beschikbaar. Denk aan het gebruik van beveiligde verbindingen, domeinnaambeveiliging en het tegengaan van phishing. Het gebruik van moderne internetstandaarden helpt cybercriminaliteit te voorkomen; het gebruik van verouderde protocollen is onveilig.

Hoe zit het met jouw domein?
Op Internet.nl kun je zien aan welke standaarden jouw website en e-mail al voldoen en waar nog ruimte is voor verbetering. Dit kan door simpelweg jouw website-URL of e-mailadres in te vullen.

TLS/SSL

Transport Layer Security (TLS) is een protocol dat de beveiliging van transport over het internet verzorgt. Dit protocol is beschikbaar voor allerlei applicatieprotocollen, waaronder HTTP (web) en IMAP (e-mail). TLS zorgt bijvoorbeeld voor het welbekende groene slotje in browsers. Vaak wordt nog gesproken over SSL, de meer bekende, maar inmiddels verouderde voorganger van TLS. TLS versleutelt en ontsleutelt het verkeer bij de client en bij de server, waardoor het verkeer tijdens het transport niet door derden uitgelezen kan worden. Zowel server als client kunnen geen tot weinig invloed uitoefenen op de route die het verkeer over het internet neemt. Door versleuteling hoeven beiden geen vertrouwen te hebben in de partijen die het transport verzorgen.

De afgelopen jaren zijn veel meer websites dan voorheen met TLS beveiligd. Er is echter nog volop ruimte voor verbetering. Ook websites waar een contactformulier op staat, en dus persoonsgegevens op worden uitgewisseld, behoeven versleuteling. Een ander voorbeeld is websites waar op bepaalde pagina's (URL's) privacygevoelige informatie staat. Denk bijvoorbeeld aan iets als www.example.nl/heb-ik-een-SOA.html. Ook het aantal mailservers dat TLS ondersteunt blijft achter.

DNSSEC

DNS is een beetje het ondergeschoven kindje in de internetwereld. Onterecht, want het is een essentieel onderdeel van het geheel. Het DNS is kwetsbaar, waardoor het aantrekkelijk is voor kwaadwillenden. Zij kunnen een domeinnaam koppelen aan een ander IP-adres, oftewel: DNS spoofing. Hierdoor worden gebruikers bijvoorbeeld misleid naar een frauduleuze website. DNSSEC is er om de DNS-lookup te beveiligen. Door cryptografische handtekeningen kan een antwoord van een nameserver op 'authenticiteit' worden gecontroleerd en wordt zodoende beschermd tegen dreiging onderweg door cybercriminelen.

SPF

Sender Policy Framework (SPF) is ontwikkeld om het SMTP-protocol van meer beveiliging te voorzien. Door middel van een TXT-record in de DNS-zone geeft het aan welke mailserver(s) geautoriseerd zijn om een e-mail te versturen vanaf jouw maildomein. Zo zorgt SPF ervoor dat buitenstaanders geen gespoofde e-mail of spam van jouw maildomein ontvangen; afzendervervalsing wordt detecteerbaar gemaakt. Indien de verzendende mailserver niet in de lijst met gepubliceerde IP-adressen staat (de zogeheten SPF-records) maar toch mail verstuurt met het betreffende domein als afzender, dan wordt de mail als niet geautoriseerd beschouwd. Jouw SPF-maatregel heeft geen impact op spam of e-mail die naar jou verstuurd wordt.

DKIM

DKIM (DomainKeys Identified Mail) is een internetstandaard waarbij de verzendende server middels een 'private key' een cryptografische hash maakt. Deze hash wordt toegevoegd aan de e-mail in de vorm van een DKIM-header, een soort zegel op de e-mailenvelop. Om DKIM te bewerkstelligen moet de uitgaande en inkomende mailserver dit ondersteunen. Dit is nog niet bij alle mailproviders het geval. Vervolgens wordt er een public-private-keypair gegenereerd; een private key voor op de mailserver en een public key voor in het DNS. De ontvangende mailserver controleert de hash in de e-mail met behulp van de publieke key in het DNS.

DMARC

DMARC staat voor Domain-based Message Authentication, Reporting & Conformance. Het is een combinatie van een goed ingesteld SPF-record en DKIM-configuratie. Dankzij DMARC is het mogelijk om een beleid in te voeren rondom de manier waarop de e-mail-provider omgaat met mailverkeer waarvan niet bekend is of deze afkomstig is van het vermelde afzenderdomein. Hierdoor kan je voorkomen dat anderen mailen namens het e-maildomein van jouw organisatie. Dankzij DMARC wordt misbruik van de domeinnaam middels e-mail verminderd, of zelfs voorkomen.

DANE TLSA

DNS-based Authentication of Named Entities (DANE) is een protocol dat ervoor zorgt dat de eigenaar van een website of e-maildomein kan aangeven welk beveiligingscertificaat voor de website of mailserver valide is. De publicatie van deze informatie vindt plaats in het Domain Name System middels TLSA records. De publicatie van deze TLSA records laat zien welke certificaatautoriteit het SSL/TLS certificaat voor de website of mailserver heeft uitgegeven. Hierdoor kan worden voorkomen dat een malafide of gehackte certificaatautoriteit (denk aan DigiNotar) een certificaat uitgeeft dat vertrouwd wordt door bezoekers/gebruikers. Het is daarnaast mogelijk om specifieker door te geven wat het unieke certificaat is dat gebruikt wordt op een website of mailserver. Zo kunnen man-in-the-middle attacks voorkomen worden.

Voor DANE geldt wat voor veel van de bovenstaande protocollen geldt: de werking is pas effectief als het protocol niet alleen door de host (website/mailserver) wordt ondersteund, maar ook door de client (websitebezoeker/verzendende mailserver) wordt gebruikt.

"Dankzij DMARC wordt misbruik van domeinnaam middels e-mail verminderd"

2.8 DDoS-aanvallen afslaan hoeft niet moeilijk te zijn

DDoS-aanvallen zijn een hot topic in de media. Er bestaat voor bedrijven en organisaties waarvan de dienstverlening gelieerd is aan het internet dan ook een grote kans dat zij te maken krijgen met een DDoS-aanval. Een aanval van een cybercrimineel hoeft niet altijd te leiden tot uitval van diensten, zoals bijvoorbeeld al vaker wel het geval was bij enkele financiële instellingen. De schade is afhankelijk van de getroffen maatregelen door de aangevallen organisatie. Wel is het zo dat als een cybercrimineel echt wil, zal een aanval altijd slagen. Lukt een aanval op basis van volume niet dan wijzigt hij zijn strategie. Wel kun je jouw organisatie goed beschermen, zodat er een forse drempel ontstaat voor de cybercrimineel. Een mooi voorbeeld hiervan is de NaWas: de nationale anti-DDoS wasstraat.

Er is voortdurend een strijd gaande tussen cybercriminelen en security-experts. Mede hierdoor ontstaan er steeds nieuwe typen DDoS-aanvallen. Met deze motivatie is in 2014 de NaWas in het leven geroepen door een aantal internet serviceproviders, onder beheer van NBIP (Nationale Beheersorganisatie Internet Providers). Zodra een DDoS-aanval wordt gedetecteerd, kan de NaWas direct worden ingezet. In de wasstraat wordt het verkeer op de servers omgeleid, schoongewassen en legitiem verkeer wordt doorgestuurd naar de infrastructuur van de provider. Oftewel: het kaf wordt van het koren gescheiden. Een belangrijke doelstelling van NBIP en de NaWas is dan ook een schoon internet.

Wist je dat...

- NBIP meer dan 2.150 DDoS-aanvallen heeft afgeslagen sinds 2014?
- Er nog geen aanval is geweest die NaWas niet heeft kunnen afslaan?
- Er in 2014 gemiddeld één DDoS-aanval per twee dagen was en in 2017 ruim twee per dag?
- Nederland in de top 10 van meest aangevallen landen ter wereld staat?
- DDoS gewoon op een 'marktplaats' verkocht wordt 'as a service'?

BIT ondersteunt NBIP

BIT is al sinds het prille begin deelnemer van NBIP en was nauw betrokken bij de opzet van de NaWas. De samenwerkingen binnen NBIP zijn een goed voorbeeld van hoe een gemeenschappelijk probleem, gemeenschappelijk aangepakt kan (en moet) worden. Ook al ben je in het dagelijks leven elkaars concurrent.

2.9 Security en uw medewerkers

Naast het inregelen van allerlei technische maatregelen, is de werknemer ook een essentieel onderdeel om de informatiebeveiliging op orde te krijgen. De factor mens is namelijk nog altijd de zwakste schakel als we het hebben over security. Het gedrag van de medewerker kan vervelende gevolgen hebben voor een organisatie. Bovendien gaan zij er veelal vanuit dat de IT-afdeling het allemaal wel geregeld heeft. Enerzijds is dit begrijpelijk, anderzijds kan IT niet het onvoorspelbare gedrag van de medewerkers voor zijn. Beiden moeten hun verantwoordelijkheid pakken en hun steentje bijdragen.

Vaak gaat het om kleine slordigheden onder medewerkers, zoals het niet melden van het verlies van een gegevensdrager of een gevonden usb-stick in de werklaptop pluggen. Maar dit kan flinke gevolgen hebben. Ook hergebruik van wachtwoorden en het onbeschermd op reis meenemen van bedrijfsinformatie zijn voorbeelden van onzorgvuldigheden met grote risico's. Om hierover bewustzijn te creëren onder medewerkers, is het zaak om hen het nut en de noodzaak van informatiebeveiliging te laten inzien. Maar hoe doe je dat? Middels onderstaande maatregelen zorg je ervoor dat jouw medewerkers bewust worden van hun gedrag en daarmee verhoog je de informatiebeveiliging.

Train je medewerkers

Om verstandig te handelen in het digitale tijdperk is het cruciaal dat medewerkers getraind en opgeleid worden. Bij BIT geloven we dat bewustwording onder werknemers de veiligheid aanzienlijk verhoogt. Hierbij moet de IT-afdeling zich open opstellen. Dit betekent dat niet alleen de technische maatregelen als meer monitoring, meer virusscanners en meer firewalls een oplossing zijn. Juist de hulp van medewerkers zelf is belangrijk. Informeer hen over de ontwikkelingen op securitygebied, geef inzicht in risico's en vraag aandacht voor maatregelen. Twee keer per jaar kan al afdoende zijn. Denk bijvoorbeeld aan een korte presentatie tijdens de afdelingsoverleggen. Dit helpt de IT-afdeling ook direct een gezicht te geven binnen de organisatie. Eén ding is zeker, een bijdrage aan security begint bij bewustwording en kennis.

Neem angst voor het melden van een misstap weg

Het komt nog te vaak voor dat medewerkers een beveiligingsprobleem niet durven te melden, omdat zij simpelweg bang zijn voor de reactie van de IT-afdeling en leidinggevende. Hierdoor kan het voorkomen dat niet slechts één computer is geïnfecteerd, maar het gehele netwerk. Zorg er daarom voor dat je deze angst of schaamte wegneemt. Hoe je dat kunt doen? Heel simpel door tijdens trainingen te benoemen dat dit ontzettend belangrijk is. Daarnaast draagt een compliment over het feit dat een persoon wel naar je is toegekomen hier ook aan bij.

Beloon goed gedrag

Zoals eerder genoemd vertrouwen werknemers volledig op de maatregelen die de IT-afdeling heeft genomen en verschillende security-technologieën. Het klinkt behoorlijk schools, maar maak werknemers medeverantwoordelijk voor security door hen te belonen voor goed gedrag. Je kunt zelfs nog een stap verder gaan en het onderdeel maken van het beoordelings- of functioneringsgesprek. Door medewerkers te belonen voor bijvoorbeeld het melden van een slordigheid, worden zij gemotiveerd om bij te dragen aan de veiligheid. Een usb-stick op de parkeerplaats gevonden, een vreemde e-mail binnengekregen of rare telefoontjes? Meld het bij de leidinggevende of de IT-afdeling en word verrast met een taart voor de hele afdeling.

Zorg voor werkbare policies bij gebruik door derden

Het gebeurt aan de lopende band dat bedrijfslaptops mee naar huis gaan en vervolgens ook door familieleden en vrienden gebruikt worden. De risico's die hiermee gepaard gaan, zijn enorm. Bedrijfsinformatie kan daardoor ineens op straat komen te liggen. De meeste werkcomputers en -laptops zijn beveiligd met een wachtwoord, maar in de praktijk is het de vraag hoe efficiënt deze beveiliging is. Wachtwoorden worden bijvoorbeeld doorgegeven aan derden, waarmee zij toegang tot bedrijfssystemen en -informatie hebben. Daarom is het van essentieel belang dat er maatregelen worden getroffen die het risico beperken; de organisatie moet zorgen voor werkbare policies. Dit kan bijvoorbeeld in de vorm van gastaccounts om derdengebruik te faciliteren, al is ook dit niet zonder risico's. De maatregelen moeten vooral passen bij de manier waarop medewerkers omgaan met bepaalde data en welke beveiliging je aan deze data mee wil geven, oftewel: de mate van bescherming.

Vergeet de ex-medewerker niet

Eén van de belangrijkste risico's waar organisaties op bedacht moeten zijn, is het risico van de ex-werknemers. In de praktijk blijkt dat zij vaak jaren later nog toegang hebben tot allerlei bedrijfsaccounts. Het is dan ook cruciaal om een 'medewerker uit dienst' checklist op te stellen. Voor de beeldvorming: bij BIT is deze checklist twee pagina's lang. Door vooraf goed na te denken over de diverse stappen, voorkom je dat belangrijke zaken over het hoofd worden gezien als het moment daar is. Denk bijvoorbeeld aan toegang tot bedrijfsmail via privé-apparaten en de wachtwoorden die (naast zijn eigen) bekend waren bij deze medewerker.

2.10 Security en jouw leveranciers

Organisaties zijn veelal afhankelijk van een (flink) aantal IT-leveranciers. Voor een veilige samenwerking is het cruciaal om afspraken te maken met leveranciers en na te gaan hoe zij bepaalde privacy- en securitymaatregelen hebben getroffen. Ga ook na wat zij doen in het geval van een incident. Basisafspraken, zoals garanties en aansprakelijkheden, zijn hierbij van groot belang, maar ook governance-instrumenten zoals SLA's (Service Level Agreements), tellen mee. Hierin staan afspraken over responsetijden en oplostijden, en tevens escalatieschema's. Daarnaast is de verwerkingsovereenkomst belangrijk, waarin staat wie waarvoor verantwoordelijk is en hoe controleerbaar deze verantwoordelijkheid is. Inzicht in en grip op afspraken met alle netwerkpartijen maken deel uit van een goed securitybeleid.

2.11 'Pas-toe-of-leg-uit'-principe breder dan IT in overheid

De Lijst Open Standaarden vormt de leidraad voor de overheid met betrekking tot IT. Op deze lijst staan internetstandaarden die voor een veiliger en toekomstbestendig internet moeten zorgen. Een goed uitgangspunt, maar er zijn wel twee kanttekeningen. Allereerst geldt deze lijst alleen voor producten en diensten van € 50.000,- of meer. Als we denken aan bepaalde standaarden voor e-mailbeveiliging zoals DMARC, DKIM en SPF, kunnen we concluderen dat de diensten die met deze standaarden uitgerust behoren te zijn, bij lange na niet zo'n waarde behalen. Ook digitale veiligheid bij goedkope systemen is van belang. In onze optiek zou er geen bedrag aan moeten hangen. Daarnaast vinden wij dat het 'pas-toe-of-leg-uit'-principe niet alleen voor de overheid moet gelden, maar voor iedere organisatie.

3. Duurzaamheid: groen internet

Met de digitalisering van de samenleving neemt het belang en het gebruik van IT en data alleen maar toe. Dit betekent ook dat er een enorme druk wordt gelegd op de wereldwijde CO2-footprint. Duurzaamheid behoort volgens ons dan ook tot Internet Schoon. Het is hoog tijd om de handen ineen te slaan en samen te werken aan een groen internet.

3.1 Uitbesteden draagt bij aan duurzaamheid

Enerzijds is een datacenter een groot energiegebruiker, anderzijds gebruikt het niet meer energie dan de gecombineerde IT op eigen locaties. Sterker nog een datacenter treft zoveel maatregelen, dat juist het uitbesteden van IT-apparatuur bijna altijd duurzamer is. Waar komt dit vooroordeel dan toch vandaan? Al het energieverbruik van de apparatuur van verschillende bedrijven is binnen een datacenter geconcentreerd en valt dus veel meer op. Echter treffen datacenters duurzaamheidsmaatregelen die voor een onderneming niet haalbaar zijn. Een kostbare maatregel die procentueel beperkt energiebesparing oplevert, is voor een enkel bedrijf niet interessant en voor een datacenter met het geconcentreerde gebruik wel. Het kostenvoordeel dat het beperken van stroomgebruik oplevert is een eerste prikkel voor datacenters om duurzaamheidsmaatregelen te treffen. Een tweede prikkel is het bedrijfsimago, in een omgeving waar duurzaamheid alsmaar belangrijker wordt.

Door de schaalgrootte zijn datacenters in staat veel efficiënter met energie om te gaan dan wanneer apparatuur op locatie staat. Door die schaalgrootte is het voor datacenters veel eerder interessant om bij voortschrijdend inzicht of nieuwe technologische ontwikkelingen te investeren in energiebesparende maatregelen. Wanneer bedrijven overstappen naar datacenters, die qua efficiëntie en innovatie niet te vergelijken zijn, wordt er energie bespaard.

"Samen werken aan een groen internet"

Datacenterbranche is duurzaam

Energiezuinige maatregelen van datacenters hebben een groot effect, zeker omdat zij de IT-apparatuur van meerdere organisaties onder hun dak hebben. Er zijn tal van mogelijkheden die van een datacenter een groen datacenter maken. Een aantal maatregelen die datacenters treffen om energie te besparen zijn:

- 100% duurzaam opgewekte energie: er zijn datacenters die gebruikmaken van 100% duurzame energie.
- Servers koelen met buitenlucht: een manier om het verbruik terug te dringen, wat bij lokale IT-apparatuur vaak niet mogelijk is in verband met de constructie van het gebouw. Bij grote datacenters is dit echter wel goed mogelijk.
- Closed Cold Corridors: deze gaan efficiënter om met gekoelde lucht. Het is een gekoeld, afgesloten gangpad voor racks en andere apparatuur. Door luchtstromen te managen kan er efficiënter worden gekoeld en zijn bovendien de koelingskosten lager.
- Hergebruiken van restwarmte: door de enorme aantallen servers die warmte produceren, kan de restwarmte gebruikt worden om de overige ruimten van het pand of omliggende panden te verwarmen.
- Aggregaten op biologisch afbreekbare diesel: ieder datacenter heeft een noodplan voor eventuele stroomstoringen. Aggregaten pakken de stroomvoorziening over. Het is mogelijk om GTL te gebruiken voor deze aggregaten, wat biologisch afbreekbaar is en geen zwavel en aromaten bevat.
- Ultrasoon bevochtigen: de lucht in datacenters moet voldoende vocht bevatten en daar worden bevochtigingsinstallaties voor ingezet. Door gebruik te maken van ultrasoonbevochtiging wordt vergeleken met traditionele stoombevochtiging een energiebesparing van circa 90% gerealiseerd.

3.2 Meten is weten

Het klinkt voor de hand liggend, 'meten is weten', maar toch zien we het nog weinig gebeuren. Als organisatie is het allereerst belangrijk om verbruik te meten, zodat je inzichtelijk hebt waar je op kunt besparen. Vervolgens moet er gekeken worden waar de voorkeur qua besparingen ligt binnen de organisatie. In het kader van besparingen is er een eerste maatregel die iedere organisatie sowieso al kan treffen: schakel onnodige hardware tijdig uit.

3.3 Selecteer duurzame en energie-efficiënte apparatuur

Om duurzaam te opereren is het vanuit de IT-afdeling belangrijk om al bij de aanschaf te kijken naar bijvoorbeeld het stroomverbruik van het apparaat. Daarnaast geldt dat het soms ook voordeliger is om oude servers te vervangen, omdat deze vele malen zuiniger kunnen zijn dan de oude. Dit bespaart niet alleen kosten, maar is ook nog eens beter voor het milieu.

3.4 Circulaire economie door recycling IT-apparatuur

Nederland is een grootgebruiker van IT-apparatuur, waarbij hardware continu wordt afgeschreven en vervangen. Echter is afgeschreven IT-apparatuur uitstekend geschikt voor hergebruik en recycling. Er komt wel het een en ander bij kijken om de oude apparatuur verantwoord af te voeren, maar verscheidene organisaties zijn gespecialiseerd in het inzamelen, verwerken, bewerken en verhandelen van IT-afval, waarbij data ook op locatie vernietigd kan worden. Het recyclen van IT-apparatuur is een belangrijke zaak omdat iedereen er uiteindelijk op vooruitgaat in economisch, sociaal en ecologisch opzicht.

"Draag jij ook je steentje bij aan een schoon internet?"