INFORMATIEBEVEILIGING MAGAZINE

THEMA: Thuiswerken (deel 2)

- Menselijk schild: gebruikers als frontlinie van de organisatie
- Met de BIO bezig blijven, hoe lang?
- Column – Een kind mag zich verstoppen

JAARGANG 21 - 2021 - EDITIE 2

Speurtocht

Nicole van Deursen

De vorige uitgave had als speciaal thema thuiswerken. We raken daarover maar niet uitgepraat en daarom gaan we dit nummer daar gewoon mee door. Onze redacteur Chris de Vries ging op zoek naar het antwoord of we thuis productiever zijn. Ard Ruiter zet ons aan het denken over de stap na het thuiswerken: hybride werken, en daarbij hoort hybride compliance. Recent haalden enkele datalekken waarbij BSN's betrokken waren het nieuws. In 'Achter het nieuws' discussiëren onze redactieleden over het BSN. Wat maakt ons BSN zo bijzonder en is dat terecht? Betreffende datalekken hebben ook de discussie weer op gang gebracht waarom het invoeren van beleid, procedures, en bijbehorende gedragsverandering toch zo stroperig verloopt. In dit nummer publiceren we meerdere artikelen die relevant zijn voor dit vraagstuk. Lees bijvoorbeeld de artikelen over het overtuigen van agile ontwikkelaars, mensen als schild en organisatiecultuur, anders kijken naar leiderschap, of de artikelen over de BIO. En voor de oplettende lezers is er deze keer een speurtocht: in een artikel deelt de auteur een wachtwoord.

Nicole

IN DIT NUMMER

Rectificatie

In iB-nummer 1 2021 is de naam van Dré Lameir op de cover verkeerd gespeld. Excuses hiervoor!

Auteurs: Dave van Stein is security transformation consultant bij Xebia Security. Hij helpt organisaties met het oplossen van uitdagingen op het gebied van security, compliance en privacy in Agile en DevOps ontwikkelomgevingen. Dave is te bereiken op dvanstein@xebia.com. Edzo Botjes is antifrAgile architect bij Xebia Security. Hij houdt zich met name bezig met de invloed van menselijk gedrag in complexe systemen. Edzo is bereikbaar op ebotjes@xebia.com.

Goed nieuws voor de CISO

Krijg je organisatie mee door de business te begrijpen en te sturen op waarde

Als CISO ben je verantwoordelijk voor de beveiliging van business en IT-processen. Een duidelijke rol. Toch blijkt dat in de praktijk, door de kloof tussen security en IT-development, die rol niet zo helder is. Wanneer is deze kloof ontstaan en hoe kunnen we zorgen dat developers de waarde van security inzien?

"Je carrière is over!", hoorde Steve Katz zijn vrouw roepen. Het was 1995 en Citigroup, waar Steve net een maand werkte, kwam in het nieuws als slachtoffer van een Russische hack. Vrij snel daarna werd Steve Katz de eerste CISO ooit met een hele duidelijke opdracht: "Je weet dat we zijn gehackt en we geven je een blanco check. We willen zeker weten dat dit niet nog een keer gebeurt. We willen dat je de beste information securityafdeling ter wereld opzet" (1). Met Steves carrière is het helemaal goed gekomen; hij werd een held en legde de basis voor hoe we nu nog steeds tegen informatiebeveiliging aankijken.

Zes jaar later verzuchtte Alistair Cockburn: "Ik had nooit verwacht dat deze groep agilisten het ooit over iets substantieels eens zou worden." Een groep van 17 developers had zich net drie dagen opgesloten in een berghut om een praktische oplossing te vinden voor hun stelling: 'om succesvol te kunnen zijn in de nieuwe economie en snel het internettijdperk in te kunnen bewegen, moeten bedrijven zich ontdoen van hun bureaucratische karikaturen en ondoorzichtige processen' (2). Hoewel hun opvattingen over softwareontwikkeling enorm verschilden, was het de groep gelukt om vier basisprincipes te definiëren in het Agile Manifesto. Hiermee was de Agile-revolutie in gang gezet wat de drijvende kracht werd achter DevOps en cloud.

Hoewel, of misschien wel doordat, deze gebeurtenissen los van elkaar hebben plaatsgevonden, is hier de kloof tussen Information Security en IT-development ontstaan. Eerst werd security losgeweekt van IT-development en omgevormd tot een autonoom orgaan met eigen verantwoordelijkheden. Vervolgens is IT-development gaan versnellen met continue verandering en verbetering als mantra. Deze kloof moeten we nu zien te overbruggen. Maar hoe doe je dat? Hoe combineer je 35 jaar aan zorgvuldig opgebouwde security-zekerheden met de geplande onzekerheid van agile?

Toegevoegde waarde

Agile en DevOps dwingen een organisatie continu na te denken over toegevoegde waarde. Als ergens de toegevoegde waarde niet duidelijk van is, wordt de stekker eruit getrokken. Security is geen uitzondering en als security officer moet je leren hierop in te spelen en over na te denken. Dit blijkt in de praktijk een uitdaging voor veel risk en security professionals. Simpelweg wijzen op externe verplichtingen of een intern beleid is niet langer voldoende; je moet kunnen aangeven waarom wat je doet en vraagt noodzakelijk is.

Helaas hebben we de luxe niet om het op zijn beloop te laten. Als het over security of privacy gaat, kan het agile principe van fail fast, fail often snel desastreuze gevolgen hebben. Vandaag de dag sta je met een datalek meteen vol in de schijnwerpers. Een incident kan direct grote financiële gevolgen hebben of een zorgvuldig opgebouwde reputatie tenietdoen. Hoe zorg je ervoor dat agile developers security niet als bureaucratisch bestempelen, maar serieus nemen omdat ze de waarde ervan inzien? Simpel, zorg dat je een 'security sales pitch' hebt die de volgende elementen bevat: rust, marketing, snelheid.

Security geeft rust

Het eerste onderdeel van je pitch is 'security is een verzekering.' Security-incidenten leiden vaak tot ongepland werk zoals code herschrijven, delen van het systeem opnieuw ontwerpen of de infrastructuur wijzigen. Omdat ontwikkelteams in een agile omgeving volledig verantwoordelijk zijn voor productkwaliteit – en in DevOps ook voor Incident Response – komt dit werk voor hun rekening. Kunnen (en willen) deze teams het risico nemen dat zij hun planning om moeten gooien of hun nachtrust op moeten offeren voor het corrigeren van een security-incident? Hoewel agile verandering omarmt, geldt dat niet voor ongepland werk. Dat willen agile teams juist minimaliseren. Gebruik om je verhaal extra kracht bij te zetten een actueel verhaal, of nog beter, een gefundeerde risico-kosten analyse. Denk hierbij terug aan de kracht van de 'holy shit-factor' zoals beschreven werd in het interview met Eelco Dykstra in iB-magazine nr. 5 van 2020 (3). Linksom of rechtsom, zorg dat je je pitch op orde hebt!

Security als marketing

De hersteltijd van een incident is natuurlijk niet de enige manier om waarde uit te drukken. De gevolgschade van een security-incident kan wel eens veel meer impact hebben. Wat doe je als klanten het vertrouwen in je product verliezen en weglopen als gevolg van een incident? Het inkomen van de organisatie kan zomaar als sneeuw voor de zon verdwijnen. Klanttevredenheid is een van de belangrijkste meetpunten voor een agile team. Om succesvol te zijn in een competitieve markt is het van belang aantoonbaar beter te zijn dan de concurrent. Door vele datalekken en hacks beginnen klanten gevoeliger te worden voor de manier waarop bedrijven met security en privacy omgaan. De impact van imagoschade is daarom een argument waar agile teams gevoelig voor zouden moeten zijn. Een transparante security-aanpak is positieve reclame.

Gitlab is een sterk voorbeeld van een cultuur van radicale transparantie. Alle processen en maatregelen zijn volledig inzichtelijk en ook alle incidenten worden publiekelijk bekendgemaakt (4). Gitlab ontving veel positieve reacties op hoe zij omgingen met een incident waarbij een productiedatabase werd gewist en veel klanten hun data kwijt waren. Gitlab meldde dit meteen publiekelijk en was heel transparant over alle vervolgacties. Dit maakte duidelijk dat dit iedereen had kunnen overkomen en dat Gitlab in dergelijke situaties serieus en professioneel te werk gaat. Openheid over hoe je omgaat met security wordt steeds belangrijker als marketing. Als security officer kan je hier handig gebruik van maken - door security onderdeel te maken van de marketingstrategie, lift je mee op dit budget.

Security als snelheidskatalysator

Om ontwikkelteams volledig over de streep te trekken moeten we nog een stap verder gaan en ons richten op activiteiten die (directe, aantoonbare) waarde opleveren. Dit lijkt onmogelijk, maar de sleutel tot succes hebben we al lang in onze zak: de risicogebaseerde aanpak. Helaas is dit begrip inmiddels behoorlijk uitgehold en houdt het in de praktijk niet meer in dan statische workflows met verplichte processtappen. Het is noodzakelijk om deze aanpak grondig om te gooien.

In de loop der tijd zijn securityvraagstukken flink veranderd. Waar er voorheen vaak sprake was van puur technische vraagstukken, hebben incidenten tegenwoordig vaak gelijk een impact op bedrijfsvoering of klanten. Helaas werken veel security experts nog in een bubbel, zonder dagelijkse interactie met business en IT. Zoals ik al eerder aangaf in dit artikel, is dit de kloof die we moeten dichten. De realiteit is non-stop aan het veranderen en daar kunnen we alleen mee omgaan door echt samen te werken met de teams die daadwerkelijk risico's kunnen voorkomen. Deze samenwerking moet in ieder geval de volgende drie cruciale onderdelen bevatten:

1. **Risicoanalyses**
   Om te bepalen welke maatregelen noodzakelijk zijn moeten risicoanalyses vaak en snel worden gedaan. Een jaarlijkse business impact assessment of pentest is simpelweg niet meer voldoende. Technieken als threat modeling (5), wheels of misfortune (6) en TRIZ-analyses (7) stellen ontwikkelteams in staat om deze analyses vaak en snel zelf uit te voeren en, indien nodig, een expert in te schakelen. Hierdoor wordt het simpel om mogelijke dreigingen snel in kaart te brengen en een afweging te maken of verdere actie nodig is.
2. **Securitycultuur**
   Security experts zijn over het algemeen goed in het voorspellen van dreigingen en het zien van gaten in de spelregels. Zij zijn dus bij uitstek de aangewezen personen om teams hierin te ondersteunen. Om niet volledig afhankelijk te zijn van specialisten, is het zaak een cultuur te introduceren waarbij teams op een positieve manier worden betrokken bij security. Maak security weer leuk en toegankelijk zodat iedereen zich medeverantwoordelijk gaat voelen. Op deze manier kan de benodigde schaalgrootte bereikt worden.
3. **Automatiseer processen**
   Door de meest simpele maatregelen te automatiseren, hebben teams daar geen omkijken naar en kunnen zij zich focussen op de business. De normale technische flow door het ontwikkelproces zou ook automatisch de veilige manier moeten zijn. Vergelijk het met het ombouwen van wegen met verbodsborden, slagbomen en snelheidsbegrenzers naar een situatie met adviezen, vangrails en airbags. De beschikbare capaciteit wordt maximaal benut en ernstige ongelukken worden voorkomen. Dit vergt helaas vaak wel een flinke investering, maar zodra teams security omarmen, gaan ze er zelf mee aan de slag!

Security verkopen is cruciaal

Agile en security worden vaak gezien als twee dingen die lastig samengaan. Het is echter een kwestie van hoe je het verpakt. Agile teams willen tevreden klanten. Als agile security officer is het zaak om duidelijk te maken dat security niet een moetje is, maar juist iets waar alle stakeholders veel voordeel uit kunnen halen! (8)

Referenties

(1) https://cybersecurityventures.com/backstory-of-the-worlds-first-chief-information-security-officer/
(2) http://Agilemanifesto.org/history.html
(3) https://www.pvib.nl/actueel/ib-magazines/ib-magazine-2020-5/downloaden
(4) https://docs.gitlab.com/ee/security/README.html
(5) https://www.threatmodelingmanifesto.org/
(6) https://cloud.google.com/blog/products/management-tools/shrinking-the-time-to-mitigate-production-incidents
(7) https://www.triz.co.uk/what-is-triz
(8) https://articles.xebia.com/being-an-Agile-security-officer

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

Een kind mag zich verstoppen

In de praktijk ben ik bijna alleen maar bezig met de privacy van volwassen mensen. En met mij een hoop collega's in dit vakgebied. Als we al eens stilstaan bij kinderprivacy, dan is het vaak vanuit de vraag wanneer jongeren oud genoeg zijn om zelf toestemming te geven voor het verwerken van hun gegevens. Als het dan al eens meer uitgebreid gaat over privacy en kinderen, gaat het vaak over vieze mannen in de online wereld die kindertjes lokken door gebruik te maken van valse identiteiten. Beiden vormen een onterecht nauwe blik.

Echte gesprekken over de rol van privacy van het kind ten opzichte van de ouders en/of verzorgers, worden amper gevoerd. Maar laat een ding heel duidelijk zijn: kinderen hebben een in het Kinderrechtenverdrag vastgelegd recht op privacy. En dat recht is net zo echt als dat recht op privacy van volwassenen. Het omvat onder meer het recht op het hebben van 'geheimpjes' en een eigen (sociaal) leven. En juist die geheimen en die privéwereld hebben we te respecteren.

Op basis van dat kinderrecht op privacy is het bijvoorbeeld niet toegestaan om e-mails, berichten of appjes van je kind te lezen. En ook moet je je verre houden van het dagboek – in welke vorm die dan ook komt. Als ik dat weleens opwerp als gespreksonderwerp, doet het me zeer te zien hoe eendimensionaal er gedacht wordt. Te vaak hoor ik van ouders die continu hun kinderen tracken via apps. En telefoons die met stalkerware worden geïnfecteerd zodat ze ook nog eens op elk moment met alle vormen van communicatie kunnen meelezen. Een gechipte hond heeft meer privacy.

'Maar dat is voor hun eigen veiligheid!', hoor ik diezelfde volwassenen dan roepen. En hoezeer ik – als moeder van een prachtig kind van 13 – ook snap dat je je kinderen wilt beschermen tegen alle gevaar van de wereld, mag een dergelijk statement nooit als excuus worden gebruikt om de privacy van kinderen 100% van de tijd te schenden. Ook voor het schenden van de privacy van kinderen geldt dat je maat moet houden. Er moet een echte geldige reden zijn om de privacy te doorbreken, die moet dan ook nog eens proportioneel zijn en subsidiair (het kan echt niet anders dan op deze manier en we houden de inbreuk zo beperkt mogelijk).

Volwassenen mogen wat mij betreft wel wat beter opgevoed worden. En dit is niet alleen een oproep om je aan de wet te houden (eenieder wordt geacht de wet te kennen), maar het is vooral ook een moreel appel. Wij bevinden ons in een machtspositie ten opzichte van kinderen, wij horen voor kinderen te zorgen en horen dat naar beste inzicht te kunnen doen. En dat betekent in dit geval: ook zorgen voor respect voor de privacy. En simpelweg omdat iets kan, het tracken van een kind en het heimelijk meelezen van alle berichten, maakt niet dat het ook ethisch oké is.

"Always eyes watching you and the voice enveloping you. Asleep or awake, indoors or out of doors, in the bath or bed — no escape. Nothing was your own except the few cubic centimeters in your skull" – George Orwell, 1984

Rachel

Auteur: Rémon Verkerk is Solution Architect bij DTEX Systems en is gespecialiseerd in digitaal forensisch onderzoek. Hij houdt zich bezig met de implementatie van de DTEX-oplossing en adviseert klanten op het gebied van insider-bedreigingen. Rémon is bereikbaar via remon.verkerk@dtexsystems.com.

Menselijk schild: gebruikers als frontlinie van de organisatie

Al sinds mensenheugenis wordt de mens gezien als 'de zwakste schakel'. In het vakgebied van informatiebeveiliging is dit dan ook een veelgehoorde metafoor. Er is veel aan gelegen om de menselijke schakels te verstevigen. Veiligheidsbewustzijn verhogen en preventieve maatregelen treffen helpen, maar blijken niet toereikend.

Ik geloof dat werknemers een belangrijke rol kunnen vervullen bij het verhogen van het veiligheidsniveau. Wanneer we het menselijk gedrag bestuderen, kunnen we bekend risicovol gedrag signaleren. De uitdaging ligt hierbij in het vinden van de juiste balans tussen het vergaren van noodzakelijke gebruikersactiviteiten en het voorkomen van onnodige inbreuk op de privacy van gebruikers.

Gebruikerssystemen (`endpoints') vormen een gewild target voor cybercriminelen. Endpoints geven doorgaans toegang tot de verschillende databronnen van een organisatie en de gebruiker heeft een sleutelpositie voor wat betreft de toegang tot deze bronnen. Een gebruiker, of liever gezegd: diens account, is immers geauthentiseerd en geautoriseerd en beschikt over een vertrouwensrelatie tot data en andere systemen binnen en buiten het netwerk. Het is dit vertrouwen dat cybercriminelen misbruiken. Ze doen zich simpelweg voor als een persoon of instantie waarmee het beoogde slachtoffer vertrouwd is. Door het slachtoffer te verleiden een linkje aan te klikken in een aan hem gericht e-mailbericht, kunnen de deuren tot de organisatie ongemerkt op een kier worden gezet. Cybercriminaliteit is de laatste jaren geprofessionaliseerd en de grondigheid waarmee aanvallen worden voorbereid hebben dan ook serieuze vormen aangenomen. Het is niet ongebruikelijk dat ketenpartners in eerste aanleg worden aangevallen, alvorens het uiteindelijke doelwit op de korrel te nemen. Als de aanvaller eenmaal toegang heeft tot bedrijfsgevoelige informatie van de ketenpartner, is het een stuk eenvoudiger om toegang te krijgen tot het eigenlijke doelwit. Een ketenpartner kan ook daadwerkelijk toegang hebben tot bedrijfskritische informatie en is in voorkomende gevallen zelfs in staat om op afstand toegang te krijgen tot een netwerk. De accounts van deze rechtmatige gebruikers moeten worden beschermd. Door de activiteiten vanaf deze accounts te bewaken, kunnen afwijkende en risicovolle gedragingen worden gedetecteerd en gestopt.

Medewerkers beschermen

Medewerkers van wie het account wordt misbruikt door derden, zijn hiervan zelden op de hoogte. Multi-factor authenticatie (MFA) is nog altijd niet de de facto standaard. Wanneer dit wel het geval is, bestaat er vaak een vertrouwensrelatie met het systeem van de gebruiker, waardoor MFA niet per definitie opnieuw wordt afgedwongen. Gebruikmakend van een buitgemaakt account en de voorzieningen die binnen de omgeving gangbaar zijn (bijv. Remote Desktop, Secure Shell, Powershell, etc.) kunnen criminelen lang onopgemerkt opereren.

In de meeste gevallen zal een indringer specifieke data heimelijk naar buiten trachten te brengen. Data wordt gebundeld, gearchiveerd en veelal via versleutelde kanalen buiten het bedrijfsnetwerk getransporteerd. Wanneer een dergelijke exfiltratie opgemerkt wordt, is deze – mits de juiste loggegevens beschikbaar zijn – herleidbaar naar de gebruiker van het account. In het geval van bovenstaand voorbeeld is de rechtmatige gebruiker van dit account te goeder trouw. Uit cijfers blijkt dat datalekken veroorzaakt worden door goedwillende medewerkers die een fout maken of nalatig zijn.

Privacy

Om vast te stellen of en op welke wijze een medewerker een rol heeft gespeeld bij een incident, is vaak een uitgebreid en tijdrovend digitaal forensisch onderzoek nodig. Als forensisch specialist, spreek ik uit ervaring wanneer ik stel dat een dergelijk onderzoek een grote impact heeft op de privacy van de gebruiker. Een niet-limitatieve opsomming van gedragingen die hierbij onderzocht worden zijn: bezochte websites, inhoudelijke e-mailberichten, chatgesprekken, bestandsanalyse - zowel zakelijk als privé, et cetera. Een forensisch onderzoek vindt slechts plaats in het geval van een concrete verdenking of wanneer er sprake is van een incident. In eerste aanleg is niet altijd duidelijk welke medewerkers (lees: `gebruikersaccounts') een rol hebben gespeeld. De kans bestaat dan ook dat er onnodig veel data wordt onderzocht om tot relevante informatie te komen.

Om een kostbaar forensisch onderzoek te voorkomen is het zaak om zoveel mogelijk potentieel relevante gebruikersdata te verzamelen, voordat een incident zich heeft voorgedaan. Het is zaak je logging op orde hebben en de juiste gegevens te loggen. Zo kan een forensisch audit trail worden verkregen, die wanneer een incident zich voordoet, direct inzicht kan geven in de oorzaak en impact van het incident.

Enkele voorbeelden van gedragingen die gelogd dienen te worden zijn: bestanden printen, bestanden delen via Airdrop, bestanden uploaden in persoonlijke webmail, bestandsextensies hernoemen, processen starten in de achtergrond, etc. Correlatie van de verschillende logbronnen is noodzakelijk om context te verkrijgen. De vergelijking met een SIEM is snel gemaakt, maar alleen wanneer de juiste gebruikersactiviteit als input gebruikt wordt, kan een goed beeld worden verkregen. Pas wanneer er sprake is van duidelijke signalen van ontoelaatbaar risicovol gedrag door een gebruikersaccount wordt de vastgelegde gebruikersactiviteiten nader onderzocht. Zolang de identiteit of ander herleidbaar persoonsgegeven niet van belang is voor de triage van het

incident, wordt deze niet vastgesteld. Dit ideologisch denken kan slechts vorm krijgen wanneer aan een fiks aantal voorwaarden is voldaan. Meer en meer organisaties voelen zich echter genoodzaakt om een dergelijke maatregel te treffen.

Voorwaarden

De voorwaarden of beperkingen zullen per organisatie verschillen en kunnen zelfs per gebruikersgroep afwijken. Maatregelen dienen proportioneel te zijn: wanneer een minder zwaar middel ingezet kan worden om het doel te bereiken, moet de organisatie dit minder zware middel inzetten. Verder moet verzamelde informatie deugdelijk beschermd en versleuteld worden tijdens transport en opslag ervan. Verder moet zoveel mogelijk pseudonimisatie van de verzamelde data te worden toegepast; een proces om identificatie van gebruikers onmogelijk te maken, dan wel zoveel mogelijk te beperken.

Het pseudonimiseren van gegevens is een methode waarbij de gegevens worden omgezet naar een hashwaarde, op basis van een of meerdere zogenaamde 'sleutels'. Alleen met behulp van deze sleutels kan de gepseudonimiseerde (niet-herleidbare) data inzichtelijk worden gemaakt. Om misbruik en daarmee niet-noodzakelijke privacyschending te voorkomen is het aan te bevelen deze sleutels of delen hiervan, in beheer te geven bij twee functionarissen binnen de organisatie. Denk hierbij aan bijvoorbeeld een Chief Information Officer (CIO), Chief Human Resources Officer (CHRO) of Data Protection Officer (DPO). Door de benodigde sleutels te beleggen bij tenminste twee verschillende verantwoordelijke functionarissen, kunnen de verschillende belangen van de organisatie en medewerkers breed worden getoetst.

User Intelligence

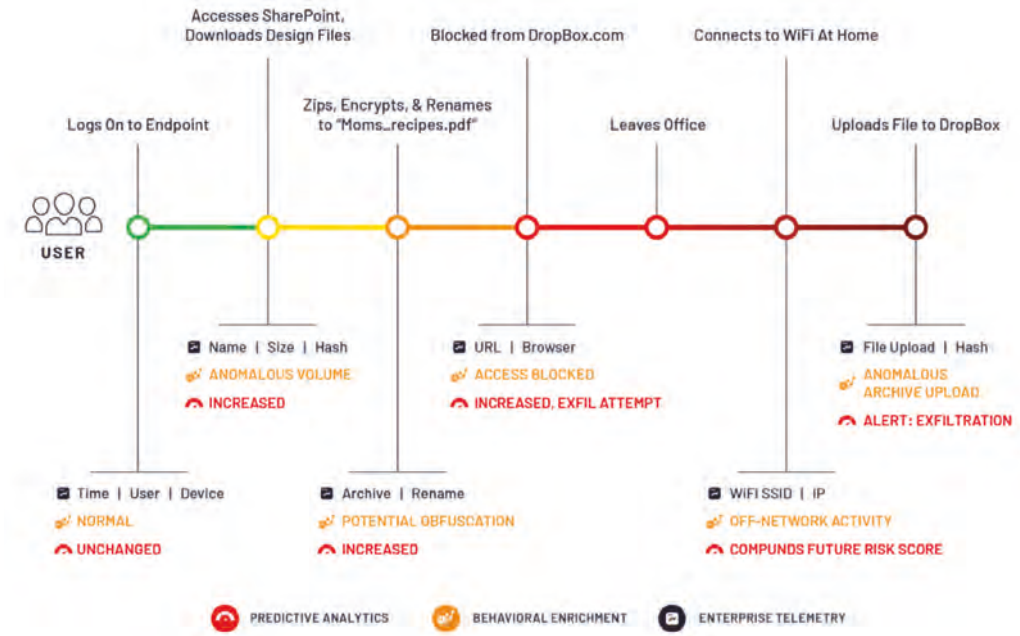
Het is van belang dat de juiste gebruikersdata verzameld wordt. Het is niet noodzakelijk of wenselijk, om de gegevens inhoudelijk te analyseren. Regulier gebruikersgedrag wordt slechts gebruikt ter bepaling van een baseline. Gedragingen worden interessant wanneer deze afwijken van de baseline van de gebruiker ten opzichte van zichzelf, van diens naaste collega's of in vergelijk met het gedrag binnen de rest van de organisatie. Een risicoscore kan het beste worden bepaald op basis van een risico-assessment voor de organisatie, waarbij de focus ligt op die gedragingen die het meest impactvol zijn. Het MITRE ATT&CK-platform (1) beschrijft de verschillende soorten tactieken, technieken en procedures (TTP's) die cybercriminelen gebruiken. Hierdoor kunnen organisaties makkelijker de gaten in hun cyberbeveiliging zien. Een voorbeeld hiervan zijn TTP's gerelateerd aan gedragingen voorafgaand of ten gevolge van, een gecompromitteerd gebruikersaccount: ongebruikelijke verhoging van privileges, domain fronting, lateral movement, omzeilen van proxy-servers, verdacht gebruik van applicaties.
Op basis van bijvoorbeeld het MITRE ATT&CK-framework kunnen profielen worden vastgesteld, waarvan de aanvalsmethodiek gerelateerd kan worden aan de vastgestelde risico's. Vermenigvuldig deze risicoscores met de mate van afwijking van bovengenoemde baselines om te komen tot een risicoscore per gebruiker. De mate van afwijking in het gebruikersgedrag kan worden vastgesteld aan de hand van een wiskundig algoritme en levert een bepaalde waarde op. Deze waarde zorgt voor een ophoging van de vooraf gedefinieerde risicoscore.

Wanneer deze risicoscore onaanvaardbaar hoog is, kan een alert worden afgegeven, waarna een analist deze beoordeelt. Op deze wijze krijgt een organisatie goed inzicht in de belangrijkste risico's voor de organisatie, waarbij de identiteit van de gebruiker afgeschermd blijft. Er kunnen aanvullende maatregelen worden getroffen, het securitybeleid kan worden aangepast en de training van securitybewustzijn van de medewerkers kan verrijkt worden met actuele dreigingen.

Context

Om alarmmoeheid (`alert fatigue') van de analisten te voorkomen en om onderscheid te kunnen maken tussen kwaadwillende, nalatige of gecompromitteerde gebruikers, is het belangrijk om samenhang te creëren tussen de verschillende waargenomen activiteiten. Aan de hand van onderstaand fictief scenario, staan we stil bij de meerwaarde van context.

Een gebruiker downloadt van Sharepoint een meer dan gebruikelijk aantal bestanden. Enige tijd later archiveert de gebruiker deze bestanden en voorziet dit nieuw gecreëerde ZIP-bestand met een wachtwoord. Voorts wijzigt hij de oorspronkelijke bestandsnaam business-designs.zip naar Moms_recipes.pdf. Twee weken later start de gebruiker zijn browser in `private browsing mode' en zet daarnaast een niet-zakelijke VPN-verbinding op, waarna hij via deze verbinding de bestanden vanaf zijn thuisnetwerk naar zijn privé-account naar de Dropbox verplaatst.



Afbeelding 1 – Een vereenvoudigde weergave van het fictieve scenario uit de tekst.

Uit het scenario blijken verschillende activiteiten die op zichzelf niet per se reden tot paniek zijn. In samenhang met elkaar valt echter op te maken dat er een relatie bestaat tussen de activiteiten en dat er duidelijk sprake is van obfuscatie, hetgeen duidt op moedwillig handelen. Zonder dat we inhoudelijk naar de data kijken, kunnen we op basis van bovenstaand contextrijke alert beslissen of er rechtvaardiging bestaat om nader onderzoek in te stellen naar dit incident en al dan niet de gepseudonimiseerde identiteit van deze gebruiker van een bepaald account te achterhalen. In de praktijk is niet ieder alert een incidentie. We moeten er echter naar streven om slechts een alert te genereren als hiervan sprake is. Door het stapelen van risicovolle gedragingen (‘alert stacking’) ontstaat context. De juiste context in combinatie met het bepalen van minimale risicoscores helpt bij het reduceren van valse positieven en het geven van prioriteit aan ontvangen alerts. Na het uitlopen van een incident waarbij de identiteit van de gebruiker zichtbaar is gemaakt, is het mogelijk om deze gegevens opnieuw te pseudonimiseren op basis van een nieuw te genereren hashwaarde.

Draagkracht

Gebruikers worden zich langzamerhand meer bewust van de gegevens die over hen worden verzameld, gebruikt en bewaard. Bovendien hebben zij in veel gevallen zeggenschap over de verwerking van hun persoonsgegevens. Naast dat wet- en regelgeving ons verplicht om transparant te zijn in de verwerking van persoonsgegevens, getuigt het van goed werkgeverschap om de hele organisatie, inclusief gebruikers, te informeren over de mate van gegevensverzameling, het doel, en de wijze waarop de integriteit en vertrouwelijkheid hiervan gegarandeerd wordt. Met de vergaring van de juiste informatie en het vertrouwen van de organisatie door het geven van transparantie bent u in staat incidenten vroegtijdig te onderkennen. Uw medewerkers vormen hierbij de frontlinie en kunnen een wezenlijke bedrage leveren aan de bescherming van de organisatie en henzelf, tegen allerhande risico’s. Beloon medewerkers met een lage risicoscore en ga in gesprek met goedwillende gebruikers die risicovol gedrag vertonen. Transparantie en samenwerking vormen de sleutel tot succes!

Referentie

(1) https://attack.mitre.org

Auteurs: Chris de Vries is een Zelfstandige Professional (ZP), waarbij informatiebeveiliging een van zijn aandachtsgebieden is en waarom hij gekozen heeft om redacteur te zijn voor dit magazine. Zijn onderneming is De Vries Impuls Management. Hij schrijft deze 'deskresearch' op persoonlijke titel en is bereikbaar onder: impuls@euronet.nl.

Thuiswerken en productiviteit

De redactie van iB heeft haar eerste nummer van dit jaar gewijd aan het thema 'Thuiswerken'. En zoals het hoort hebben wij daarbij veel aandacht besteed aan de veiligheidsaspecten daarvan. Maar, hoor ik u denken, is dat alles wat daarover te zeggen valt? Ik denk van niet, want naast de beveiliging zou ook aandacht mogen bestaan voor de effectiviteit, de efficiëntie en de rentabiliteit van het thuiswerken.

Het was in de jaren 80 van de vorige eeuw dat op de Erasmus Universiteit de vraag gesteld werd wat opbrengsten en kosten eigenlijk zijn, welke inspanningen leiden wel tot opname onder de opbrengsten dan wel kosten, en welke niet? Daarbij werd als opvallend voorbeeld het werk van de huisvrouw aan de orde gesteld. Toen gold nog dat haar werk waardeloos was – ik hoor(de) de storm van protesten toen al –, dus noch opbrengst noch kosten. Dat standpunt kwam voort uit de Nationale Rekeningen in aansluiting op de internationale richtlijnen (1). En de visie kwam weer voort uit de onmogelijkheid (wil?) om de prestaties van huisvrouwen te waarderen vanwege het ontbreken van prijsbepaling op een formele markt waar vraag en aanbod elkaar zouden kunnen ontmoeten.

En nu werken wij allen thuis! Toch krijgen wij loon, want de plaats van werken blijkt niet relevant te zijn. Wat natuurlijk wel een rol van betekenis voor onze werkgevers speelt (2), is dat wij even productief of productiever zijn. En wat weten wij van deze productiviteit?

In het navolgende, vergelijk ik Nederlandse publicaties over dit thema met een actuele publicatie van het Leibniz-Zentrum für Europäische Wirtschaftsforschung (ZEW) (3) alsook een `oude' Engelse publicatie (12).

TNO-onderzoek

RTL-nieuws meldt onder het thema: `Werkplezier' naar aanleiding van een onderzoek van TNO (4), dat `tussendoor de hond uitlaten', ons creatiever en productiever maakt. Dit na waarneming van 850 met name hoger opgeleiden, die meerdere keren per week invullen hoe ze zich voelen in de TNO-app HowAmI. Na een trage start, veroorzaakt door de noodzakelijkheid de ICT-problemen op te lossen, steeg de productiviteit snel en zelfs tot hoogten boven werken op kantoor. Dit gekoppeld aan hogere creativiteit en het hebben van positieve gevoelens, maakt dat TNO concludeert dat de productiviteit is gestegen. Als nadelen zag het TNO de combinatie van thuiswerk en thuiszittende kinderen, het vinden van een juiste werk-privé tijd balans en het ontbreken aan een zekere regelmaat om elkaar fysiek op kantoor te ontmoeten. Op 18 september 2020 rapporteerde TNO vervolgens dat voor zes van de tien werknemers het werk door COVID-19 is veranderd en dat het de veerkracht bewijst van de ruim 10.000 onderzochte werknemers. De bevindingen: 44% werkte drie maanden na de start thuis, waarvan circa 65% volledig, met name hoogopgeleiden in de leeftijdsgroep van 25 tot 54 jaar en vooral werkend in de ICT en de financiële dienstverlening (5). TNO onderzocht ook de effecten op werkdruk en het ervaren stressniveau. De werkdruk lag net iets boven de 10% (NEA-COVID-19 meting), het percentage thuiswerkers met burn-outklachten op 17%. Beide percentages zijn stabiel ten opzichte van 2019. Bij het stressniveau zijn er echter grote verschillen, zeker deels veroorzaakt door het moeten combineren van werken thuis met zorgtaken, zoals de kinderen in thuisonderwijs, daar vragen vooral de jongere kinderen veel meer aandacht.

Navraag bij de werknemers leert dat circa 25% ook na corona thuis wil blijven werken. Van 14% van de werknemers die nog niet (volledig) thuiswerkt, is bekend dat zij dat wel wil. Er is dus vraag naar. TNO stelt wel dat er grote verschillen bestaan tussen de sectoren. Werknemers constateren dat er nog het nodige moet worden gedaan aan de werkplek (45%) en dat men veel meer achter het beeldscherm zit. Positieve effecten: afname ongewenst gedrag, (CdV: nog?) geen toename in de fysieke en mentale klachten (6).

PriceWaterhouseCoopers

PwC constateert dat er aanmerkelijke baten te behalen zijn door thuiswerken (7). Zij becijfert het cumulatieve voordeel op € 7,8 miljard en dat komt onder meer voort uit bespaarde huisvesting- en kantoorkosten, het positief saldo tussen lagere kosten woon-werkverkeer en de hogere energierekening thuis (CdV: een besparing voor de werkgever!), minder verkeersongevallen, minder investeringen in infrastructuur en vermindering van de CO_2-uitstoot.

Daar staan tegenover: bedrijfscultuurverandering, dubbelzinnige effecten m.b.t. innovatief vermogen, ziekteverzuim, productiviteit, het niet altijd kwantificeerbaar zijn van de effecten (CdV: doet mij denken aan het thuiswerken van de huisvrouw) en de ongelijke verdeling van de kostenbesparingen tussen werkgever en werknemer.

Saillant is dat op 29 oktober 2010 PwC er nog ervan uitging dat "(te) veel thuiswerken organisaties mettertijd € 1,5 miljard kan kosten" (8). Zij baseerde dat toen op de factoren: minder samenwerking, isolatie en stress, de kosten voor de werkgevers

gecombineerd met een hoger verloop, ziekteverzuim en lagere productiviteit.
Recruitment adviseur Robert Walters publiceerde op de website dat productiviteit toeneemt bij thuiswerkende werknemers (41%) en dat zou overwegend beaamd worden door de werkgevers. Daarbij zijn 553 hoogopgeleide professionals in Nederland onderzocht en net als TNO constateren zij een hogere toename bij partners zonder kinderen. De toename wordt met name verklaard door de flexibele werktijden waardoor werknemers beter hun eigen bioritme kunnen volgen. Ook het wegvallen van de reistijden en minder vergaderingen wordt als positief ervaren, terwijl de afleiding van het werk sterk persoonlijk gekleurd wordt en wel of niet invloed uitoefent. In ieder geval wil 85% van de werknemers ook in de toekomst regelmatig thuiswerken (9).

StakeholdersLab (blog)

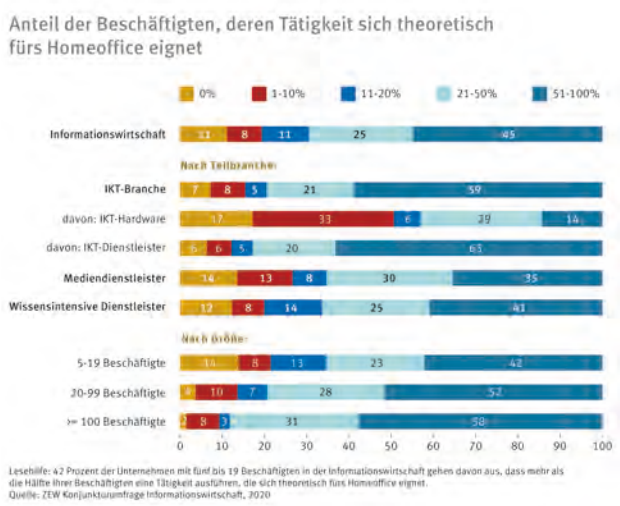
Er zijn echter ook kritische geluiden. In het blog 'Thuiswerken maakt millennials onproductief' van het StakeholdersLab (10), calculeert de auteur dat er 2,3 miljoen onderpresteerders zijn op een totale beroepsbevolking van 9,2 miljoen (11). Het onderzoek is gebaseerd op de uitkomsten van een meting van de Nationale Thuiswerk Monitor in september 2020.

Binnenlands Bestuur

Ook in het online magazine Binnenlands Bestuur spreekt auteur Hans Bekkers zijn zorg uit met betrekking tot de productiviteit van de overheid als gevolg van het moeten thuiswerken van ambtenaren. De oorzaken zijn in dit artikel niet uitgewerkt en lijken gebaseerd op de aanname dat thuiswerken leidt tot een onvermijdelijk verlies aan productiviteit. Persoonlijke opvattingen en de eigen ervaring met thuiswerk lijken daar de doorslag te geven. Dit bleek uit een zogenoemd Flitsonderzoek van het programma Internetspiegel/vensters van het ministerie Binnenlandse Zaken en werd op internet gepubliceerd op 25 maart 2020 (12).

Duitsland

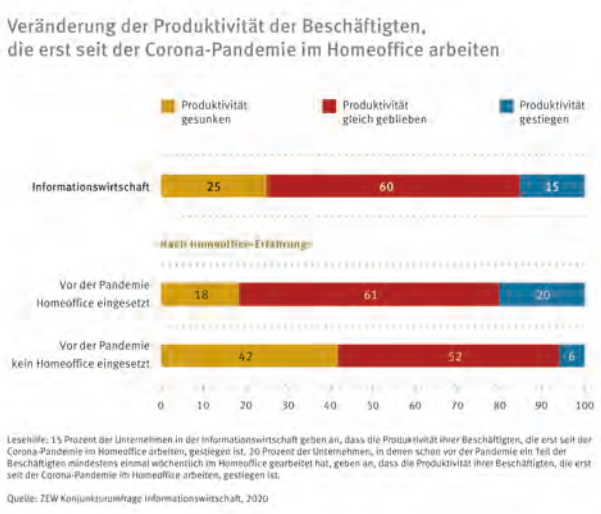
Duitsland is voor ons een van de belangrijkste handelspartners en in vele opzichten lijken onze landen erg op elkaar en zijn onze economieën sterk verweven. Wat is de Duitse visie op de productiviteit van thuiswerken? Ik ben eens te rade gegaan bij het toonaangevende Zentrum für Europäische Wirtschaftsforschung (ZEW, opgericht in 1990), dat zich richt op twee belangrijke thema's: politiek relevant onderzoek en wetenschappelijk gefundeerde advisering van de politiek.
Op 8 februari 2021 publiceerde dr. Daniel Erdsiek (wetenschapper in het onderzoeksgebied Digitale economie) een artikel met de titel: 'Hohes Homeoffice-Potenzial in der Informationswirtschaft' (Informatie Economie) (3). Dat artikel is gebaseerd op een enquête (december 2020) onder circa 850 Duitse bedrijven, waarbij naar boven kwam dat liefst 45% uit deze sector meent dat meer dan de helft van haar werknemers goed thuis zou kunnen werken. Liefst 75% van die werkgevers stelde vast dat hun medewerkers een gelijke of hogere productiviteit hadden.



Afbeelding 1 – Aandeel werknemers en werkzaamheden geschikt voor thuiswerken.

Zoals bovenstaande afbeelding aantoont, verschilt het percentage van geschiktheid per sector, maar het geheel beoordelende is de constatering dat er zeer positief gedacht wordt over de mogelijkheden van thuiswerk.
Ter verduidelijking deze sector omvat de Informatie – en Communicatietechniek (IKT-Dienstleisters), media- en kennis(intensieve) servicebureaus, maar ook juridische- , belasting-, consultancy-, architectuur-, ingenieur-, reclame- en marketingbureaus c.q. –bedrijven. En heel logisch constateert men ook in Duitsland dat de hardware leveranciers/producenten veel lagere kansen inschatten om werk thuis te laten verrichten. Ook is logisch dat de grotere ondernemingen positiever zijn dan de kleinere ondernemingen.

Wat de productiviteit betreft, toont deze sector over veel vertrouwen te beschikken dat deze zich minstens op eenzelfde niveau zal handhaven (60%), terwijl 15% zelfs een stijging in productiviteit waarneemt, ook bij die werknemers die voor het eerst thuiswerken. Niet onvermeld moet blijven dat 25% van de ondernemers wel een terugval in productiviteit ervaart. Als oorzaken voor de negatieve productiviteit worden genoemd de technische infrastructuur thuis, de implementatie van het thuiswerken en de zorg voor de kinderen door de sluiting van scholen en kinderdagverblijven.



Afbeelding 2 - Productiviteitsverandering bij werknemers met eerste keer ervaring thuiswerken.

Als belangrijkste oorzaak van deze ontwikkelingen stelt de onderzoeker dat de snelle verandering van de arbeidsorganisatie niet mogelijk maakte dat deze overgang goed gepland kon worden. Het is handelen in/tijdens een crisis. Conclusie: zij die al ervaring hadden met thuiswerken konden de productiviteit doen stijgen of gelijk houden (CdV: effect van autonomie, eigen werktijd indeling, positieve ervaringen, thuiswerktips en dus een gevolg van een ervaringsvoorsprong!?). Eindoverweging van dr. Erdsiek: zouden de ondernemers die niet eerder thuiswerk hadden toegestaan wellicht hun oordeel laten kleuren door hun mogelijk sceptische visie op dat thuiswerk en de invloed daarvan op de arbeidsproductiviteit?

Verenigd Koninkrijk

In Engeland viel mijn oog op een onderzoek van de Universiteit van Birmingham dat dateerde van 24 april 2017 (13). De onderzoekers constateerden destijds al dat autonomie met betrekking tot de werkplek positieve effecten sorteerde ten aanzien van welzijn en functietevredenheid. Het betrof hier een Understanding Society-onderzoek onder 20.000 werknemers. Zij zagen verder dat het beroep en de sekse een grote rol bij de beoordeling speelden.

Destijds was de volgorde van afnemende welzijn en tevredenheid onder werknemers van hoog tot lager niveau: managers – professionals – andere werknemers – laaggeschoolden. Ook destijds scoorden de informele flexibiliteit en het thuiswerken positief, waarbij het met name vrouwen waren die hier meer belang aan hechtten dan mannen. Of dit het gevolg is/was van een meer masculiene cultuur in het Verenigd Koninkrijk dan hier te lande, kan ik niet bevestigen of ontkennen. Dat dit een rol van betekenis her en der in de wereld speelt is wel zeker. Zoals de onderzoeker het formuleerde: "Flexibility in work location, specifically homeworking, benefitted women with caring responsibilities allowing them to better manage paid work alongside the household". Ook hier het onterechte onderscheid tussen betaald werk en de 'waardeloze' werkzaamheden thuis. Verder moet worden opgemerkt dat in het Verenigd Koninkrijk geen parttimebanencultuur bestaat zoals in Nederland. Veel werkgevers laten mensen pas na enkele jaren dienstverband minder uren werken en dat bemoeilijkt voor hen de combinatie tussen zorgtaken en werk. De uitspraak van de onderzoeker getuigt dus van die werkcultuur.

De belangrijkste reden - in dit pro-corona tijdvak - voor managers om daar niet aan toe te geven is omdat die managers het als hun belangrijkste taak zagen om in controle te blijven en de inspanningen van werknemers te bewaken (CdV: lees productiviteit).

Dit Engelse onderzoek vat eigenlijk wel aardig de hiervoor beschreven ontwikkelingen samen. En ook hier wederom het 'vrouwenthema'!

Mijn conclusie

Ik meen dat Chinezen hun vijanden interessante tijden toewensen. Nu dan, wij leven in een interessante tijd met haar oorzaak in China. Corona heeft door haar aard een onvoorziene disruptie veroorzaakt, die het noodzakelijk maakte in isolatie te gaan en tegelijkertijd de samenleving en de

Dus corona is wellicht een 'blessing in disguise'

economie draaiende te houden.
Dit hebben wij in Europa met veel flexibiliteit en creativiteit gedaan en thuiswerken is met één klap het nieuwe normaal geworden. De werknemer heeft de kans gekregen autonomie te behouden, het zou de niet werkende partner de gelegenheid kunnen bieden om hun arbeidsprestatie gewaardeerd te krijgen en dat bedoel ik niet alleen ten aanzien van het huishoudelijk werk! De werkende partner moet opeens mee opvoeden, onderwijzen en het huis op orde houden.
Ook is nu opeens de techniek van vergaderen en bijeenkomen veranderd. Ik zal vanaf nu veel minder beurzen of klanten bezoeken, en vergaderen via de apps zal gemeengoed worden. Ik zal dus minder kilometers afleggen en daarmee bijdragen aan een lagere CO_2-uitstoot in afwachting van het betere alternatief dan de huidige elektrische auto.
Voorgaande onderzoeken hebben zich vooral gericht op de hoger opgeleiden en dat kan een vertekenend beeld opleveren. Lager opgeleiden en millennials kunnen een minder belang hebben bij thuiswerken en hun werk kan zich (deels) daarvoor minder lenen. Mijn effectiviteit en efficiëntie ervaar ik in ieder geval als verbeterd. Dus corona is wellicht een 'blessing in disguise'. Echter met mate te genieten, er ontstaan mogelijkerwijs lifestyle- of gezondheidsdilemma's en wij moeten er rekening mee houden dat culturele verschillen hun invloed zullen uitoefenen op hoe onze 'buren' (Europees, Engels, Amerikaans, Russisch, Chinees enz.) daar mee omgaan en onze oplossingen zullen accepteren.
Vanuit ons vak gezien zullen er in eerste instantie meer informatiebeveiligingsrisico's ontstaan, maar als Europa het goed oppakt, ook nieuwe en betere kansen voor ons in een wereld waar de kenniseconomie doorslaggevend zal zijn. Ik kijk in ieder geval positief naar de toekomst.

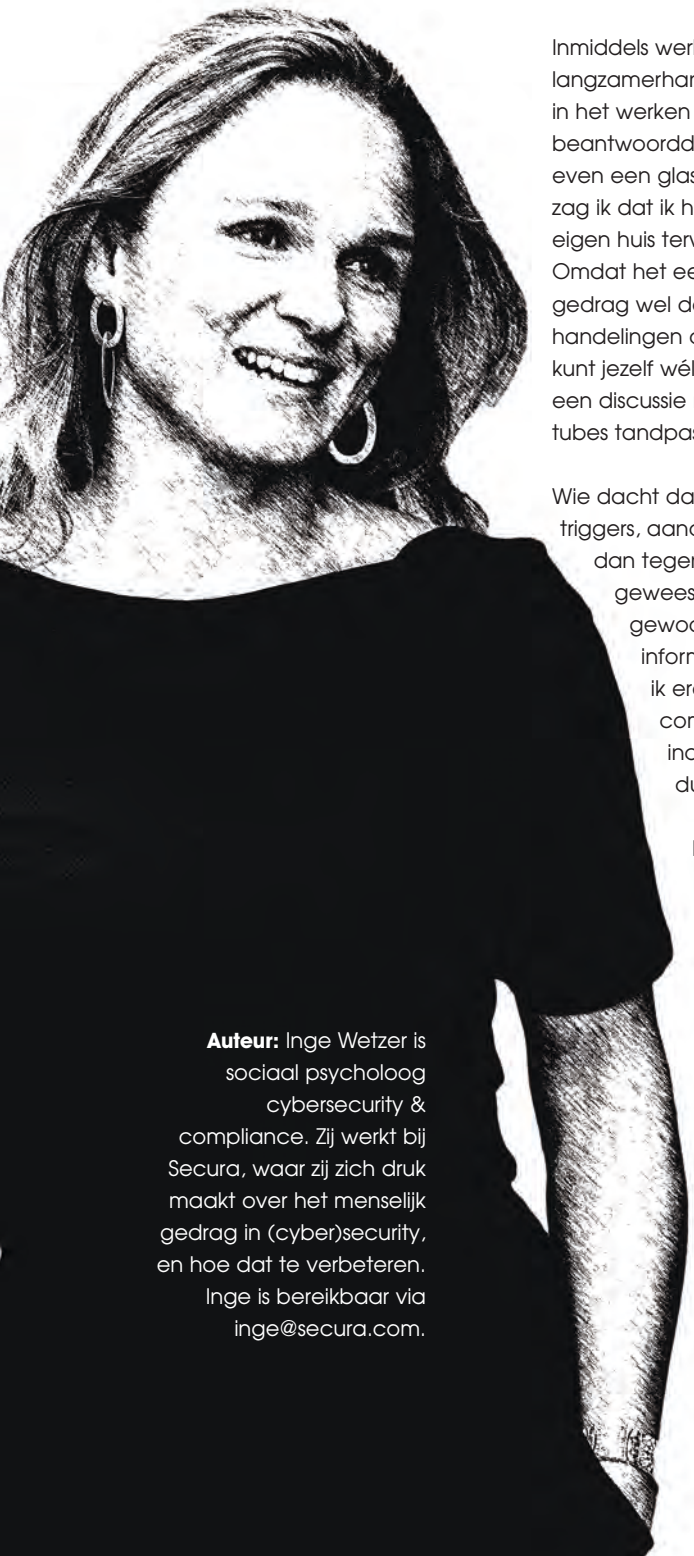
Tips voor thuiswerken

Voor hen die eenvoudige tips willen hebben voor het productief thuiswerken, bezoek eens de website van Omgevingsweb (13).

Referenties

(1) Nationale Rekeningen 1980, CBS – Staatsuitgeverij 08.1981, pagina 49: 'Goederen welke door de consument zelve in en speciaal ten behoeve van de eigen huishouding worden voortgebracht zijn als regel noch in de nationale produktie noch in de consumptie begrepen. Dit laatste geldt voor de werkzaamheden van huisvrouwen in de huishouding en ook voor de opbrengst van volkstuintjes.' (CdV – Aardig toch die toevoeging van de volkstuintjes!?)
(2) (CdV – Opdrachtgevers sluit ik even uit, want opdrachtnemers werken als zelfstandige professionals toch vaak vanuit een thuissituatie en als ze wel op een locatie van de opdrachtnemer werken, dan zijn en blijven ze autonoom, want zodra er sprake is van een gezagsverhouding dan is er ook sprake van arbeidsovereenkomst en dat is wat de opdrachtgever niet wenst).
(3) https://www.zew.de/presse/pressearchiv/hohes-homeoffice-potenzial-in-der-informationswirtschaft
(4) https://www.rtlnieuws.nl/economie/life/artikel/5171464/thuiswerken-werkgeluk-tno-vertrouwen d.d.16.07.2020 (10:39 uur)
(5) https://www.tno.nl/nl/over-tno/nieuws/2020/9/voor-6-op-de-10-werknemers-is-het-werk-veranderd-door-corona-maatregelen/ d.d. 18.09.2020; mede gebaseerd op NEA-COVID-19 onderzoek uitgevoerd ultimo juni tot ultimo juli 2020
(6) https://www.tno.nl/nl/over-tno/nieuws/2021/2/kwart-thuiswerkers-na-corona-deels-thuis-blijven-werken/
(7) https://www.pwc.nl/nl/actueel-en-publicaties/themas/economie/de-baten-van-thuiswerken-zijn-aanzienlijk.html
(8) https://www.pwc.nl/nl/actueel-en-publicaties/themas/economie/te-veel-thuiswerken-kan-op-termijn-anderhalf-miljard-kosten.html
(9) https://www.robertwalters.nl/hiring/hiring-advice/41-procent-werknemers-productiever-bij-thuiswerken.html
(10) http://www.stakeholderslab.nl/blog-thuiswerken-maakt-millennials-onproductief/
(11) https://www.binnenlandsbestuur.nl/financien/nieuws/corona-crisis-schaadt-productiviteit-overheid.12729186.lynkx?tid=TIDP319329X315A4F61E44C41DE821AE040CB2282E3YI5
(12) https://www.birmingham.ac.uk/news/latest/2017/04/autonomy-workplace.aspx
(13) https://www.omgevingsweb.nl/loopbaan/7-tips-voor-productief-thuiswerken-tijdens-corona/?utm_medium=social&utm_source=email&utm_campaign=Artikel+gedeeld

Nooit te oud om te leren



Inmiddels werk ik, zoals zoveel anderen, alweer maanden thuis. We zijn er langzamerhand een beetje aan gewend geraakt en hebben onze draai gevonden in het werken op afstand. Zojuist ontdekte ik bij mezelf een interessant patroon: ik beantwoordde wat mailtjes en wilde daarna aan deze column beginnen. Eerst nog even een glas water halen beneden. Toen ik weer boven bij mijn computer kwam, zag ik dat ik hem had gelockt. Haha! Ik lock tegenwoordig dus mijn computer in mijn eigen huis terwijl ik één minuut weg ben. Omdat ik denk dat dat nodig is? Nee. Omdat het een automatisme is geworden. Yes! Ben ik zelf ineens het bewijs dat nieuw gedrag wel degelijk aan te leren is. En dat het automatiseren van sommige handelingen dus zeker wel mogelijk is. Ook als je al heel wat jaartjes meedraait. Je kunt jezelf wél dingen anders aanleren! Die zin mag je onderstrepen en gebruiken in een discussie met je partner of kinderen over rondslingerende sokken, dopjes op tubes tandpasta of openstaande deuren.

Wie dacht dat-ie te oud is voor gedragsverandering, heeft het mis. Met de juiste triggers, aandacht en moeite zijn wij mensen heel flexibele wezens. Misschien sta ik dan tegenwoordig wel bekend als 'Miss Cyberveilig gedrag', dat is niet altijd zo geweest … Er waren jaren dat ik mijn computer niet altijd lockte, maar soms gewoon wegliep. Pas toen ik mij ging specialiseren in het vak van informatiebeveiliging, vond bij mijzelf ook de omslag plaats. Ten eerste kwam ik erachter dat het veel sneller kan dan via Ctrl + Alt + Delete – Lock computer: gewoon de Windowstoets (linksonder op het toetsenbord) indrukken en dan tegelijk op de L (van lock) drukken. Windows + L(ock) dus. Deze ontdekking maakte het al een stukje makkelijker.

Daarnaast werd ik ook gemotiveerd tot ander gedrag; ik werkte in een omgeving die cybersecurity ademde. Tussen mensen die veiligheid in hun genen hadden en onveilig handelen als een zonde zagen, waarbij je op zijn minst flink moest trakteren als je daarmee de mist in ging. Ik kon dus al gauw niet meer anders. In het begin was dat vooral een kwestie van alert zijn en blijven nadenken. Maar als je een nieuwe handeling maar vaak genoeg bewust herhaalt, ga je dat gedrag dus langzaam automatiseren. Ongeacht je leeftijd. Dus in het begin was het heel bewust, maar al gauw werd die nieuwe handeling automatisch. Zo automatisch, dat ik dus blijkbaar niet meer van mijn stoel op kan staan zonder Windows + L in te typen. Dat is eigenlijk één beweging geworden: ik sta op dus ik toets Windows + L in. Zelfs als ik alleen thuis ben.

Inge

Auteur: Inge Wetzer is sociaal psycholoog cybersecurity & compliance. Zij werkt bij Secura, waar zij zich druk maakt over het menselijk gedrag in (cyber)security, en hoe dat te verbeteren. Inge is bereikbaar via inge@secura.com.

Auteurs: mr. A.IJ. (Ard) Ruiter werkt als privacy- en beveiligingsfunctionaris/senior inspecteur bij de ILT Inlichtingen- en Opsporingsdienst (ILT-IOD). Hij schreef dit artikel op persoonlijke titel en is bereikbaar via LinkedIn.

Security overwegingen bij hybride werken

Door de coronamaatregelen stond veel plotsklaps op zijn kop. Ook voor de thema's informatiebeveiliging en cybersecurity. Opeens hadden vele medewerkers gevoelige data beschikbaar in (minder beveiligde) privéwoningen. Een aantal overwegingen voor een veilige informatie(t)huishouding bij hybride werken.

Het afgelopen jaar is voor een belangrijke mate gevormd door het 'severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2)' dat de ziekte COVID-19 kan veroorzaken. Het jaar zat ook vol met initiatieven die overheden, bedrijven en particuliere ondernemingen om thuiswerken mogelijk te maken. Van de ene op de andere dag werd massaal thuisgewerkt. De corona-maatregelen hebben geleid tot het grootste veldexperiment in de informatietechnologie ooit. Velen werken thuis en zijn al maanden niet op een kantoor geweest; ook bij bedrijven waar geproduceerd moet worden, wordt meer informatietechnologie ingezet. De digitaliseringsgolf en het digitaal bewustere gedrag van mensen heeft er in ieder geval voor gezorgd dat de economie bleef draaien.

Van kantoor via thuiswerken naar hybride werken

De uitdrukking 'Je werk mee naar huis nemen' heeft een heel andere betekenis gekregen. Het gaf aan dat je de uitdaging van het werk juist niet op kantoor liet en thuis geen mogelijkheden meer zag om in alle rust van quality time kan genieten. In deze tijd gaat het er om dat werk mee naar huis nemen niet automatisch betekent dat je niet tot rust komt, maar bij juiste indeling in tijd en afgrenzing van de privémomenten ook verrijkend kan zijn en de productiviteit kan stimuleren. Nu vindt veel werk thuis plaats waarbij de werkomgeving mixt met de privésfeer. Al het thuiswerken was zo'n kleine tien jaar geleden volstrekt ondenkbaar. De sindsdien razendsnelle technologische ontwikkelingen maken dat nu mogelijk. Thuiswerken met gevoelige informatie werd voorheen niet geschikt geacht en ook telewerkvoorzieningen waren nog niet geheel adequaat. Het lijkt alweer lang geleden, maar begin 2020 hadden we nog de Citrixaffaire (1). Door dit beveiligingslek was digitaal thuiswerkwerken tijdelijk onmogelijk. De patches werden snel beschikbaar gesteld (2). Voorafgaand aan vrijdag 13 maart 2020 golden strengere maatregelen tegen de verspreiding van het coronavirus; opeens was thuiswerken de norm. Het gebruik van telewerkvoorzieningen werd in rap tempo normaal. Alle technologiedeskundigen staken veel effort in het faciliteren van het 'nieuwe normale' werken: alle middelen in de informatie- en communicatietechnologie (ICT) en met name inlogsoftware moesten perfect gaan functioneren. Bij de informatievoorziening gaat het immers om het geheel van mensen, middelen, informatiesystemen en maatregelen, die zich allen richten op de specifieke informatiebehoefte van een organisatie en haar medewerkers. Deze informatiebehoefte bevat gegevensverzamelingen, procedures, processen en programmatuur en alle voorzieningen voor opslag, verwerking en communicatie voor die informatiesystemen.

Plaatsonafhankelijk

Telewerken verandert structureel het werken in de toekomst. De pre-coronatijd-behoefte aan kantoorlocaties wordt minder (3). Er komt minder verkeer en waarschijnlijk een grote spreiding in werktijden. Werken wordt een combinatie van vaste fysieke ontmoetingsruimten, werkplekken die je ergens onderweg kunt boeken, thuiskantoren en virtuele werkomgevingen. Deze 'plaatsonafhankelijke arbeid' is mogelijk via Wireless Fidelity (WiFi)/ Wireless-Local Area Network (W-LAN) of via 4G en straks zelfs 5G. In hybride – of wellicht nomadische – werkculturen is voor de werklocatiekeuze niet het kantoor leidend, maar het type werk, het type gerubriceerd of geclassificeerde informatie (4), het doel van de activiteit, de gewenste mate van interactie, de efficiëntie van communicatie en de persoonlijke voorkeuren van medewerkers enerzijds en 'klanten' burgers, consumenten, hulpzoekenden, cliënten, leerlingen, afnemers, etc. anderzijds (5). Binnen de samenleving en alle organisaties vinden ontwikkelingen plaats die te maken hebben met het toenemend gebruik van ICT, digitale informatie, data en informatiesystemen. Wat zullen de (nieuwe) vereisten voor security en informatiebeveiliging zijn, als medewerkers documenten van de ene naar de andere plek en vice versa meenemen? Informatiebeveiliging is immers het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen. Let wel, het is ongeacht waar die systemen en/of de gebruikers zich bevinden. Informatiebeveiliging op zichzelf is dus ook plaatsonafhankelijk geworden en moet dus 'overal' worden ingevoerd. Informatiebeveiliging zal dan meer worden bezien in het kader van de integrale veiligheid voor het selecteren, implementeren en periodiek evalueren van een samenhangend stelsel van beveiligingsmaatregelen voor de beveiliging van belangen op basis van risicomanagement.

Securitytips voor thuiswerken

De grootste winst van het thuiswerken is een betere werk-privé-balans en meer focus op de werkzaamheden. De beleving van thuiswerken verschilt wel, vooral naar levensfase (6). Voor veilig thuiswerken moeten – aanvullende – beveiligingsmaatregelen worden getroffen. Op vele sites zijn goede tips te vinden om de informatiebeveiliging goed in te richten bij het thuiswerken, zie kader.

Hybride werken en data/privacy compliance

Nu geldt alweer een jaar lang voor iedereen het uitgangspunt 'thuiswerken, tenzij …' Er zijn ook al vele (tussen)evaluaties

Tips voor veilig thuiswerken

- agentschaptelecom.nl/onderwerpen/telekwetsbaarheid/blogs/thuiswerken-door-het-coronavirus
- autoriteitpersoonsgegevens.nl/nl/nieuws/veilig-thuiswerken-tijdens-de-coronacrisis
- cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus_0.pdf
- domaintools.com/resources/blog/covidlock-mobile-coronavirus-tracking-app-coughs-up-ransomware
- dnvgl.nl/news/18-tips-voor-informatiebeveiliging-thuiswerken-tijdens-covid-19-185083#
- dnvgl.nl/news/veilig-thuiswerken-informatiebeveiligingstips-voor-werkgevers--185087
- ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-gebruik-tweefactorauthenticatie
- ncsc.nl/onderwerpen/phishing/weerbaar-tegen-phishing
- ncsc.nl/documenten/publicaties/2019/mei/01/wifi-onderweg-gebruik-een-vpn
- ncsc.nl/onderwerpen/veilig-thuiswerken
- ncsc.nl/onderwerpen/veilig-thuiswerken/documenten/publicaties/2020/april/1/factsheet-uw-thuiswerkfaciliteiten-zijn-nu-onmisbaar
- recordedfuture.com/coronavirus-panic-exploit
- rivm.nl/coronavirus/covid-19
- us-cert.gov/ncas/alerts/aa20-073a

Voor tips en tests die helpen een thuiswerkplek te verbeteren voor je eigen lichaamshouding en de verbinding te optimaliseren: consumentenbond.nl/thuiswerken.

uitgevoerd. Daaruit blijkt dat thuiswerken wel zeker een blijvertje zal zijn. Hybride werken zal een combinatie worden van werken op drie 'plekken':

1. De kantoorwerkplek: voor een ieder bekend en vaak formeel, strak georganiseerd;
2. De (mobiele) thuiswerkplek met een corporate device of een private device: dat kan thuis, maar ook op een bezoek bij (groot)ouders of (klein)kinderen, vakantiepark of wellicht vanuit de kajuit van een zeilboot in de passantenhaven van Terschelling;
3. De mobiele werkplek: van thuis (waar dat ook mag zijn) naar kantoor en vice versa.

Dat betekent ook dat informatie op twee manieren verwerkt zal worden:

1. Digitale verwerking in de laptop van het werk of digitaal door met een privé device in te loggen op het bedrijfsnetwerk;
2. Fysieke verwerking in documenten. Nog steeds zullen vele dossiers, overeenkomsten, afspraken, ontwerpen, tekeningen en andere 'printjes' worden verplaatst, al dan niet met rubricering van de informatie.

Thuiswerken en hybride werken zijn onlosmakelijk verbonden met het meenemen van data buiten het controleerbare (beheersbare?) kantoorterrein. Hybride werken brengt daarom nieuwe uitdagingen met zich mee met betrekking tot de maatregelen, normen van de informatiebeveiliging, de compliance en gedragsregels 'op papier' van de organisatie alsook het gedragsconforme, feitelijke werken van de medewerkers. Het vraagt ook de aandacht van privacy en compliance officers. Deze bedrijfsmedewerkers kunnen zich niet het recht toe-eigenen om een woning te betreden om te controleren of de medewerker zich wel aan de discretierichtlijnen van de organisatie houdt.

Evaluaties van thuiswerken

- agconnect.nl/blog/drie-stappen-naar-een-veilige-thuiswerkplek
- agconnect.nl/artikel/thuiswerken-voelt-voor-werknemers-toch-niet-als-toegestaan
- computable.nl/artikel/achtergrond/magazine/7110421/5215853/computable-onderzoek-thuiswerken-is-blijvertje.html
- rekenkamer.nl/publicaties/publicaties/2020/11/02/focus-op-digitaal-thuiswerken
- rekenkamer.nl/actueel/nieuws/2020/11/02/digitaal-thuiswerken-bij-de-rijksoverheid

Privacyfilters

Onder 'normale' omstandigheden wordt gereisd met laptops en werken 'we' op meerdere locaties. Wanneer gevoelige informatie wordt verwerkt, moeten encrypted laptops worden gefaciliteerd met gateways en line encryptors. Daarvoor kan de afspraak gemaakt worden dat we laptopschermen beschermen met zwarte privacyfilters, zodat derden niet kunnen meekijken. Bij thuiswerken kan het theoretisch gebeuren dat de buren door het raam op het scherm meekijken. Ook voor die schermen zou een privacyfilter moeten komen. Maar een privacyfilter houdt niet alles tegen. Voor de verwerking van bepaalde bedrijfskritische informatie en bedrijfsgeheimen, ligt het in de lijn der verwachtingen dat het management in die gevallen de medewerker verplicht om de data alleen in een afsluitbaar vertrek van een kantoorpand te houden: thuis- en hybride werken is dan zelfs verboden!

Juridisch lekken

Als een willekeurige derde alleen al meekijkt op het scherm met persoonsgegevens die de organisatie verwerkt, dan moet dat juridisch worden gezien als het verstrekken van persoonsgegevens door de organisatie. Het begrip 'verstrekken van persoonsgegevens' moet ruim worden opgevat: het omvat iedere vorm van het bekendmaken of ter beschikking stellen van persoonsgegevens, ongeacht de wijze waarop dit gebeurt. Het kan mondeling, schriftelijk of langs elektronische weg gebeuren maar ook door bij het overhandigen van een magneetband met gegevens. Ook het raadplegen van gegevens, bijvoorbeeld op cd-rom, valt onder verstrekken. Van verstrekken is ook sprake als een persoon over de schouder van een ander meekijkt naar bijvoorbeeld een bestand persoonsgegevens (7). Kortom, onachtzaamheid met het omgaan van ICT-middelen met persoonsgegevens door een medewerker op een andere locatie dan het kantoor, kan juridisch al betekenen dat de medewerker informatie 'lekt'.

Fysieke documenten thuis en onderweg

De vraag rijst of een (digitale) kopie kan/mag worden gemaakt voor thuiswerken. Er mogen niet meer kopieën gemaakt worden dan strikt noodzakelijk. Ingewikkeld criterium in de praktijk. Geëist zou kunnen worden dat de kopieën van unieke exemplaarnummer worden voorzien en geregistreerd. Maar mag gerubriceerde informatie via de e-mail worden verstuurd? Bestaat daarvoor een secure line? Is elke organisatie voldoende geëquipeerd om goedgekeurde, geëvalueerde cryptomiddelen in te zetten?

Een andere leuke overweging is de vraag of papieren informatie verstuurd moet/mag worden naar woningen. Een criterium zou kunnen zijn om fysieke informatie uitsluitend buiten gecontroleerd gebied te brengen indien dit voor de voortgang van de werkzaamheden noodzakelijk is en de manager toestemming heeft verleend. De organisatie zal de risico's moeten afwegen in zijn algemeenheid, maar ook voor het ene document in het bijzonder. Van belang zal zijn dat de transporteur geen inzage mag hebben of mag kunnen verkrijgen in de informatie. De Postwet 2009 impliceert dat het 'eenieder verboden is een ongeopende brief die bestemd is per post te worden bezorgd en niet voor zichzelf bestemd is, te openen en te lezen zonder toestemming van degene aan wie de post wel gericht is'. Geldt dit alleen voor 'papieren' brieven, of zijn hier aanvullende, redelijke maatregelen nemen om te voorkomen dat de informatie in verkeerde handen valt? Dat kan via organisatorische, technische of contractuele maatregelen.

Bewaren en vernietigen

En mag die informatie dan thuis worden bewaard? Waarschijnlijk zal een organisatie kunnen besluiten om het bewaren van fysieke documenten of informatiedragers uitsluitend toe te staan in een goedgekeurde kluis in een ruimte met inbraakalarmering; misschien zelfs in een inbraakvrij vertrek in een privéwoning. De vraagt dringt zich op of een werkgever de mogelijkheid heeft dit af te dwingen. Wie draagt eigenlijk op voor de kosten? En wat te doen met de ingebouwde kluis van de werkgever als de medewerker een promotie krijgt bij een andere (concurrerende) organisatie? Ook die thuis bewaarde bedrijfsinformatie zal aan bewaar-, verwijderings- en vernietigingstermijnen gebonden zijn. Dus dat betekent vernietigen. Mag de medewerker dat thuis doen of moet het worden teruggestuurd naar kantoor ter vernietiging? En hoe gaat de compliance officer daar toezicht op houden?

Focus op digitaal thuiswerken

De Algemene Rekenkamer onderzocht tussen juli en oktober 2020 welke ICT-middelen de medewerkers van ministeries en Hoge Colleges van Staat gebruiken, waarvoor zij die gebruiken, welke beveiligingsrisico's dit oplevert en hoe de organisaties hun beleid hierover communiceren.

In zijn rapport 'Focus op digitaal thuiswerken' (8) wordt een aantal concrete voorbeelden met risico's genoemd. Zoals werknemers die de organisatie verlaten, maar in app-groepen blijven meelezen met werkgerelateerde (vertrouwelijke) informatie. Er wordt geïnvesteerd in het communiceren van gerubriceerde informatie, maar daar staat tegenover dat sterk beveiligde faciliteiten in de praktijk weinig worden gebruikt omdat ze niet makkelijk in het gebruik zijn. Populaire berichtenapps, tablets en smartphones hebben de voorkeur, boven de sterk beveiligde middelen omdat ze gemakkelijker, sneller en gebruiksvriendelijker zijn. Medewerkers maken soms behalve de

aanbevolen middelen ook gebruik van alternatieve ICT-samenwerkingsplatformen. Een afdoende niveau van informatiebeveiliging en privacy is daarbij niet vanzelfsprekend en veel organisaties zijn zich hiervan bewust. Het is vrijwel onmogelijk te controleren welke ICT-samenwerkingsplatformen medewerkers precies gebruiken. Soms is gebruik van een 'ontraden' middel zelfs onontkoombaar, dan wordt vaak een beroep gedaan op gezond verstand: bewustzijn en werken aan de hand van principes in plaats van harde regels. Een beroep op gezond verstand: bewustzijn van de medewerker, de intrinsieke betrokkenheid bij de materie en werken aan de hand van principes in plaats van harde regels. 'Het zou helpen als de gebruiker zich meer bewust is van de gevaren van het delen van informatie via bepaalde bronnen. Het lijkt mij belangrijk dat we werken vanuit verantwoordelijkheid in plaats van het naleven van regeltjes' (9).

'De coronacrisis bracht digitaal werken (…) vanaf maart 2020 in een stroomversnelling. Dit vergde een enorm aanpassingsvermogen van tienduizenden medewerkers en tientallen ondersteunende diensten. Ambtenaren moesten een permanente thuiswerkplek inrichten, tegelijkertijd vaak in beslag genomen door thuisonderwijs voor hun kinderen en zorgen over kwetsbaren in hun omgeving. Ondersteunende diensten zetten alle zeilen bij om de ICT-infrastructuur overeind te houden bij het enorme aantal thuiswerkers en om verzoeken om ondersteuning van medewerkers af te handelen' (10).

Design

Goed is, om ook te kijken naar goede mogelijkheden in het ontwerp van informatiesystemen. Secure/security by design betekent dat softwareproducten vanaf de basis zijn ontworpen om veilig te zijn. Ook kan er ruimte zijn voor de privacy-by-design-ontwerpfilosofie (11). Deze vereist dat privacybescherming vanaf het begin af aan meegenomen wordt bij het ontwerpen en bouwen van nieuwe systemen. Privacy is een software kwaliteitsattribuut. Ontwerpers sturen de eerste ontwerpschetsen in een privacyvriendelijke richting, door in het begin te dwingen weloverwogen principiële keuzes te maken. Nieuwe technieken vereisen een aanpassing in gebruik en gedrag. De toegepaste technologische mogelijkheden kunnen in dat kader ethisch verantwoord worden ontworpen. 'Design ethics' betreft moreel gedrag en verantwoorde keuzes in de ontwerppraktijk. Met 'ethical design' is daarom een ontwerp gemaakt met de bedoeling om goed te doen. Er zullen heroverwegingen zijn over het begrip privacy bij het verwerken van persoonsgegevens. Nieuwe beveiligingsmaatregelen op gegevens ontstaan bij opslag, transport en tijdens de verwerking.

Hybrid compliance thinking

Prachtig dat we nu met al die prachtige ICT-middelen thuis kunnen werken en hybride kunnen werken. Het wordt nog een uitdaging voor de governance en de compliance en conduct policymakers om de privacy en informatiebeveiliging goed te waarborgen. Er zullen nieuwe denklijnen gaan ontstaan en daarmee ook een hybrid compliance thinking. De tijd is aangebroken om risico's en kansen inzichtelijk en systematisch te inventariseren en te beoordelen. Welke maatregelen zullen die risico's beheersbaar maken? We zitten in een spannende en uitdagende periode en met hybrid compliance thinking gaan we een eind komen. Niets is moeilijk voor zij die willen (12). De toekomst zal ons het begrip leren en dat begrip kunnen we inzetten voor de verdere ontwikkeling van veilig hybride werken. Citaat van de Deense filosoof Søren Kierkegaard (13): "Het leven kan alleen achterwaarts begrepen worden, maar het moet voorwaarts worden geleefd."

Referenties

(1) publiekdenken.nl/nieuws/i-samenleving/lessen-uit-citrix-affaire/
(2) ncsc.nl/actueel/nieuws/2020/januari/19/update-advies-patches-citrix
(3) nos.nl/nieuwsuur/artikel/2366749-grote-werkgevers-gaan-na-corona-kantoorruimte-schrappen.html en nos.nl/nieuwsuur/artikel/2366750-
(4) Classificatie zorgt ervoor dat duidelijk is welke data en systemen belangrijk zijn, de zogenaamde kroonjuwelen, en welke minder belangrijk. Gesteld wordt dat meest gebruikte methode (BIV) minder objectief is dan het lijkt; Klaverda, P., Kuiper, R., 'Een andere kijk op classificatie, Informatiebeveiliging Magazine, 2020, nr. 4, p. 4-6
(5) Zie o.a: Wat is hybride werken? - Management Impact; managementimpact.nl/artikel/wat-is-hybride-werken/
(6) Bijma, B. 'Hoe beleven we thuiswerken in coronatijd? 6 lessen' SERMagazine, 15 oktober 2020, ser.nl/nl/Publicaties/thuiswerken-coronatijd-lessen
(7) Zie Mvt bij de Wbp; https://zoek.officielebekendmakingen.nl/kst-25892-3.html en Registratiekamer, 6 maart 1995, 94.V.177
(8) Algemene Rekenkamer (2020). Focus op Digitaal thuiswerken. Den Haag, Kamerstukken II 2020-21, 35420, 181
(9) Algemene Rekenkamer (2020), a.w., p. 11
(10) rekenkamer.nl/actueel/nieuws/2020/11/02/digitaal-thuiswerken-bij-de-rijks-overheid
(11) Hoepman, J.H. (2020) 'Privacyontwerpstrategieën (Het Blauwe Boekje)', Nijmegen/ Groningen: De Privacy Coach, cs.ru.nl/~jhh/publications/pds-boekje.pdf
(12) Nil volentibus arduum
(13) Søren Kierkegaard (1813-1855), origineel citaat: "Livet forstås baglæns, men må leves forlæns" Blanken, G.J. Kierkegaard. Een inleiding in zijn leven en werk, Amsterdam (Ambo), 2012

2021

Het jaar is alweer begonnen met een aantal spraakmakende cybersecurity onthullingen die ons werkgebied weer op de kaart hebben gezet. Zoals de hacks bij SolarWinds en bij een waterzuiveringsinstallatie in Florida.

Informatiebeveiliging is dus weer volop in het nieuws en je kan je afvragen of dit goed of slecht nieuws is. Feit is wel dat dit soort nieuws helpt om aan te tonen dat ons werk noodzakelijk is en dat bedreigingen niet imaginair zijn. Tevens zijn berichten van uitgebreide analyses van de hack in de meer gespecialiseerde blogs en nieuwssites een belangrijke bron om beter te begrijpen wat de echte threats nu zijn, en welke maatregelen je moet nemen om je hiertegen te wapenen. Een goede manier om bij te blijven in je vakgebied.

Vanuit het bestuur kijken we ook naar onder andere deze stroom van informatie en vragen we ons af of wij als PvIB hier iets mee moeten doen. De vereniging vervult nu al een behoefte met het iB-Magazine en de vele events die onze leden beiden zeer waarderen. We beseffen dat dit een groot goed is, dat we zeker moeten behouden, vernieuwen en versterken waar mogelijk. Maar ook hierbij vragen we ons af of je nóg relevanter voor de leden en de samenleving kan zijn. En natuurlijk hoe je dat vormgeeft in een vereniging waar een relatief kleine groep vrijwilligers de taken uitvoert en die dit, naast hun bestaande baan, met veel liefde en passie doen. Hoe kunnen we andere PvIB-leden verleiden om zich in te spannen voor het vakgebied maar ook voor hun eigen ontwikkeling? We zijn geïnteresseerd in jullie ideeën, aangezien we jullie nodig hebben, om met behoud van het karakter van de PvIB, ons klaar te maken voor de toekomst.

Erwin Bosma
secretaris@pvib.nl

Auteur: Dennis Teuben, University of Applied Science, dennis.teuben@student.hu.nl.

Horizontaal toezicht vanuit privacy by design

Persoonsgegevens zijn een vorm van data en in veel gevallen privacygevoelig. The Economist stelde in 2017 dat niet langer olie, maar data de meest waardevolle grondstof ter wereld is (1). Helaas zien we regelmatig dat het niet goed gaat met de bescherming van privacy bij de verwerking van persoonsgegevens. De schade is groot en soms zelfs onmogelijk te herstellen. De recente datalekken in de GGD-registratiesystemen bij de bestrijding van de coronapandemie is hier een pijnlijk actueel voorbeeld van (2).

Door het datalek kwamen persoonsgegevens van miljoenen Nederlanders, tot het burgerservice nummer (BSN) aan toe, op straat te liggen of in handen van criminelen. Een dergelijk datalek is niet alleen bijzonder schadelijk voor de GGD zelf, maar ondermijnt ook het vertrouwen in een betrouwbare overheid. Gevolg daarvan is dat Nederlanders terughoudender worden om zich te laten testen op het coronavirus, wat een daadkrachtige bestrijding van de epidemie niet ten goede komt. Voorkomen is dus beter dan genezen.
Of het nu gaat om de registratiesystemen van de GGD of de borging van privacy in politiesystemen (3), privacy is hot. Uit het Tweede Kamerdebat rond de toeslagenaffaire kwam onder andere naar voren dat het toezicht op de verwerking van persoonsgegevens te wensen overlaat. Hier werd een verwijt gemaakt naar de toezichthouder, de Autoriteit Persoonsgegevens (AP), maar dat is misschien niet helemaal terecht. De AP heeft te maken met een enorm capaciteitstekort en kan daardoor bijna alleen reactief handelen, en niet preventief optreden. Er is nauwelijks tijd om organisaties te adviseren over compliance. Na de melding van een datalek, die regelmatig uit de organisaties zelf komt, kan de AP een onderzoek instellen. Wat betreft het daadwerkelijke toezicht is de AP allerminst een tandeloze tijger. Vanaf 25 mei 2018 moeten alle organisaties die met persoonsgegevens werken voldoen aan de Algemene Verordening Gegevensbescherming (AVG). De AVG heeft alleen betrekking op de verwerking van persoonsgegevens binnen EU-grondgebied of als de verwerking gaat over onderdanen van de Europese Unie (EU). De AVG is een set van regels om de privacyrechten van natuurlijke personen te beschermen. In het geval van non-compliance kan een toezichthouder een boete opleggen van ten hoogste 20 miljoen euro of van maximaal 4% van de wereldwijde jaaromzet van de organisatie. Dat de AP daadwerkelijk boetes oplegt, bleek onlangs nog toen het OLVG in Amsterdam een boete van 440.000 euro opgelegd kreeg (4).

Onderzoek

We zien de grote waarde van persoonsgegevens en het gebrek aan compliance en aan de andere kant een toezichthouder die door gebrek aan capaciteit niet voldoende in staat is toezicht te houden om het vertrouwen in een betrouwbare overheid gestalte te geven. In mijn onderzoek, onder supervisie van Dr. Bas van Gils aan de University of Applied Science Utrecht, stel ik de vraag hoe enerzijds compliance in informatiesystemen beter geborgd, anderzijds hoe het toezicht hierop effectiever en efficiënter ingezet kan worden. Het onderzoek is naar verwachting dit voorjaar voltooid.
De Belastingdienst is in 2005 begonnen met zogenaamd Horizontaal Toezicht (HT). Een toezichtmethode die de van oudsher sterk hiërarchische toezichtrelatie meer wil inrichten op basis van samenwerking. Horizontaal toezicht kenmerkt zich door het principe van 'voor wat, hoort wat'. De uitgangspunten zijn begrip, wederzijds vertrouwen en transparantie. De inherente onvoorspelbaarheid en machtsongelijkheid, die zo kenmerkend is voor klassieke toezichtrelaties, wordt hierdoor beperkt. Horizontaal toezicht heeft ten doel om toezicht naar voren te halen en het proces te vereenvoudigen (5). De introductie van horizontaal toezicht past ook bij een ontwikkeling waarbij wordt gezocht naar alternatieve toezichtvormen om de beperkte toezichtcapaciteit van de Autoriteit Persoonsgegevens efficiënt in te zetten. Horizontaal toezicht wordt ingezet om toezichthouden vanuit wantrouwen om te buigen naar toezichthouden vanuit vertrouwen. Zelfregulering en meer verantwoordelijkheid aan organisaties zijn hier producten van (6) en passen ook bij de mate van verantwoordelijkheid zoals wordt genoemd in art. 26 AVG.

Voordelen horizontaal toezicht

Huiskers concludeert dat horizontale toezichtrelaties goed kunnen werken voor grote organisaties: 'Zij zijn minder gevoelig voor de machtsmiddelen, zoals boetes en naheffingen, en voegt eraan toe dat hoe groter de organisatie, hoe grotere de behoefte bestaat aan zekerheid. En juist deze zekerheid kan in een horizontale toezichtrelatie snel geboden worden. Een organisatie weet dan relatief snel dat zij compliant zijn m.b.t. de verwerking van persoonsgegevens. Huiskers benadrukt dat het voordeel van een horizontale toezichtrelatie is dat aan de voorkant van het proces het toezicht plaatsvindt en niet achteraf, als het spreekwoordelijke kalf al verdronken is. Horizontaal toezicht is echter niet gratis. Het vraagt vanuit de organisatie en de toezichthouder een duidelijke motivatie om tot een bestendige horizontale toezichtrelatie te komen. Door gelijkwaardige én wederkerige interacties tussen partijen ontstaat er vertrouwen. Vertrouwen leidt tot transparantie en verbeterde processen. De toezichthouder kan goed gedrag belonen met het verlagen van de toezichtdruk. Dergelijke beloningen werken als een olievlek en kunnen andere organisaties motiveren om beter te presteren. De energie die in horizontaal toezicht moet worden gestoken

Nr.	Principe	Toelichting
1	Proactief niet reactief – preventief niet repressief	PbD geldt vanaf de initiatie van het ontwerp van een systeem en niet achteraf.
2	Privacy als standaardinstelling	Privacy criteria gelden per default. Daarbij is de regel "comply or complain".
3	Privacy geïntegreerd in ontwerp	Privacy maatregelen zijn integraal onderdeel van de informatieverwerking en zijn geen toevoeging.
4	Volledige functionaliteit	Het waarborgen van de privacy is een verantwoordelijkheid van alle betrokken partijen.
5	End-to-end beveiliging	PbD waarborgt het privacy management, inclusief de beveiliging, gedurende de gehele levenscyclus van de persoonsgegevens. Het is geen eenmalige actie.
6	Zichtbaarheid en transparantie	Inzicht en transparantie over de verwerking van persoonsgegevens moet mogelijk zijn voor zowel het individu als de eigen organisatie en toezichthouders.
7	Gebruiker staat centraal	Technische en organisatorische maatregelen zijn pas effectief, wanneer zij de persoonlijke levenssfeer van het individu beschermen.

Tabel 1 – Privacy by design principles, Cavoukian, A. & Others (2009).

vraagt echter ook capaciteit, dus het is te makkelijk om te stellen dat er alleen maar capaciteit gewonnen wordt.
Horizontaal toezicht vraagt om een controle-instrument dat in de organisatie aanwezig is en ervoor zorgt dat compliance geborgd wordt. De toezichthouder kan dan vertrouwen op de werking ervan. In het kader van mijn onderzoek ontwerp ik een privacy control framework (PCF) dat ervoor moet zorgen dat zowel privacy compliance als horizontaal toezicht gefaciliteerd worden. Dit PCF is ontworpen aan de hand van de in 2009 door Cavoukian (7) ontwikkelde principes van Privacy by Design (PbD), zie tabel.

Conclusie

Privacy is zeer actueel en persoonsgegevens bijzonder waardevol. Om privacy te borgen moet er reeds bij de ontwikkeling en bij het gebruik van informatiesystemen nagedacht worden over compliance. Een privacy control framework op basis van de principes van privacy by design kan hiervoor worden ingezet. De andere kant van de medaille is dat er effectief toezicht gehouden moet worden door de Autoriteit Persoonsgegevens. Door gebrek aan capaciteit vindt dit thans bijna uitsluitend reactief plaats. Een moderne toezichtrelatie in de vorm van horizontaal toezicht kan hierbij wellicht uitkomst bieden. Dit vraagt van zowel de onder toezicht staande organisatie als de toezichthouder wel een inspanning. De samenwerking begint bij het aangaan van het gesprek. Pas dan kan toezicht, gebaseerd op wantrouwen worden omgebogen naar een gelijkwaardige relatie op basis van vertrouwen.

Referenties

(1) https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data
(2) https://www.volkskrant.nl/nieuws-achtergrond/datalek-bij-ggd-gegevens-van-miljoenen-nederlanders-in-criminele-handen~b7f17bea/
(3) https://www.bitsoffreedom.nl/2020/11/19/ict-systemen-politie-niet-op-orde-iedereen-de-dupe/
(4) https://autoriteitpersoonsgegevens.nl/nl/nieuws/ziekenhuis-olvg-beboet-om-onvoldoende-beveiliging-medische-dossiers
(5) Huiskers, E., & Gribnau, J. (2019). Cooperative Compliance and the Dutch Horizontal Monitoring
Model. Journal of Tax Administration, 5(1), 66–110
(6) Raaijmakers, K. (2016). Inherente onvoorspelbaarheid in toezichtrelaties. Jaarboek Compliance 2016, 65–79
(7) Cavoukian, A., & others. (2009). Privacy by design: The 7 foundational principles. Information and
Privacy Commissioner of Ontario, Canada. Retrieved from https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

COLUMN Berry

Weg, die telefoon

Jullie kennen Berry natuurlijk van zijn enthousiaste verhalen over techniek en over hoe mooi het allemaal wel is met de komst van internet, de mobiele telefoon, en alles elektronisch te kunnen doen en de effecten op de samenleving.

De winkelstraten zijn leeg doordat bol.com en andere grootwinkelbedrijven goedkoper zijn. De snelst groeiende groep criminelen zijn de mensen die goed met een toetsenbord om kunnen gaan. Deze groep wordt weleens afgebeeld als langharige slonzige mannen met dikke baarden die de hele dag cola drinken, maar niets is minder waar. Deze mensen zijn tegenwoordig gewoon gekleed in driedelig grijs, goed opgeleid en georganiseerd.

Inmiddels heeft Berry zijn werk ingeruild voor een plek waar de automatiseringsgraad een stuk lager ligt. Ik vervul daar een leidinggevende positie en kom zo nu en dan in een situatie terecht die ik mij eerder niet kon voorstellen. Hiervan een voorbeeld.

In ons gebouw komen veel mensen en op een bepaald moment krijg ik een appje van een collega die aangeeft een coronabesmetting te hebben. Heel naar voor haar, maar ik dacht eigenlijk direct aan de andere collega's. We spraken af dat iedereen zich laat testen en aangeeft wat de uitslag was. Een paar dagen later komt een collega binnen en vraagt mij te helpen. Hij is getest maar heeft niets van de GGD gehoord. Ik doe mijn mondkapje beter op en vraag hoe ik kan helpen. Hij zegt dat de site van de GGD niet goed werkt. Ik zoek de site op en geef aan dat hij kan inloggen met zijn DIGID-app. `Ja maar, ik heb geen mobiel, alleen een vaste lijn en daarmee valt de sms-authenticatie af. Niet getreurd, je kunt ook inloggen met je identiteitskaart, alleen: die functie geeft een storing. Bellen lukt ook niet. Ik kan niet anders dan hem naar huis te sturen in afwachting van de uitslag. Hij is weg en ik denk na over bestellen bij online winkelbedrijven, betalen van je rekeningen, invullen van je belastingen, het uitlezen van je zonnepanelen en noem maar op. Zoals hij zijn er veel meer mensen die op die manier proberen hun `ding' te doen. Het is een generatie die het internet gemist heeft en dat overigens heel bewust doet. Die niet de hele dag naar WhatsAppberichten wil kijken of Facebook wil checken. Daar zit natuurlijk wel wat in. Het geeft misschien ook wel de rust die ik nu soms als onrust ervaar. Maar om te wachten op een telefoontje dat maar niet komt en niet in staat zijn om zelf te bellen, geeft mij weer onrust. Nee, ik hou het maar zoals ik het nu heb.

Berry

Auteur: Ing. Ruben Zeegers CISSP CIPM CBP werkt als security consultant bij Security Risk Watch. Tevens is hij oprichter van bio-training.nl. Dit artikel is geschreven op persoonlijke titel. De heer Zeegers is bereikbaar via: ruben.zeegers@securityriskwatch.com.

BIO, een worsteling of geschenk?

Informatiebeveiliging binnen de Nederlandse overheid valt onder de Baseline Informatiebeveiliging Overheid (BIO). Deze standaard is voor de overheid verplicht. Maar hoe geef je hier binnen jouw organisatie nu praktisch invulling aan? En hoe zorg je ervoor dat jouw organisatie kan aantonen hieraan te voldoen?

De BIO heeft per 1 januari 2019 de bestaande baselines informatieveiligheid voor Rijk (BIR), Gemeenten (BIG), Waterschappen (BIWA) en Provincies (IBI) vervangen. Hiermee is er een gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid gekomen. De BIO is gebaseerd op de ISO27001/2, de internationale standaard voor informatiebeveiliging. In de landelijke media zien we steeds vaker berichtgeving over incidenten waarbij overheidsorganisaties betrokken zijn. Organisaties worden bijvoorbeeld slachtoffer van ransomware, datalekken en fraude met financiële en/of reputatieschade als gevolg. Als security consultant begeleid ik publieke en private organisaties met het verder professionaliseren van informatiebeveiliging en privacy. Regelmatig krijg ik van opdrachtgevers vragen zoals: "We hebben al veel maatregelen getroffen maar voldoen die ook aan de BIO? Welke BIO maatregelen moeten we nog meer treffen? Hoe kunnen we aantonen dat we BIO compliant zijn? En wat als er toch een groot incident voorvalt?" Om deze vragen te kunnen beantwoorden moeten we eigenlijk een paar stappen terug doen. Vooropgesteld, incidenten zijn nooit 100% te voorkomen. Wat we wel kunnen doen is: risico's beheersbaar maken. Dit houdt in dat we zo veel mogelijk incidenten proberen te voorkomen en wanneer zich toch een incident voordoet, proberen de gevolgschade zo veel mogelijk te beperken. We treffen technische, organisatorische en fysieke maatregelen op basis van organisatie specifieke risico's. In het kort is dit het doel van het managen van informatiebeveiliging. De BIO zelf is dus geen doel maar een hulpmiddel om hieraan invulling te geven. Een instrument waarmee informatiebeveiliging wordt vereenvoudigd, gestructureerd en aantoonbaar gemaakt voor de Nederlandse overheid.

Kennis

Om dit instrument goed te kunnen bedienen is kennis over informatiebeveiligingsprincipes van essentieel belang. Ik zit in overleggen waarbij de betrokken business eigenaar bijvoorbeeld niet weet wat de term 'risico' precies inhoudt. Wanneer je met een business eigenaar een BBN-toets doet, moet je dit wel kunnen uitleggen. Anders kom je op een dwaalspoor, loop je vast en worden risico's onjuist geclassificeerd. En zo zijn er binnen de BIO nog veel meer informatiebeveiligingsprincipes waarbij kennis van het doel en de werking nodig is om er invulling aan te kunnen geven. Hierbij valt onder andere te denken aan gap-analyse, eigenaarschap, ISMS, bewustwording, incident management, verantwoording en ketensamenwerking. Wanneer al deze onderdelen goed worden ingevuld en in samenhang zijn, ontstaat er een mate van informatiebeveiliging die robuust is en voldoende bescherming biedt. Hierdoor wordt er aan de eisen van de BIO voldaan. Wanneer er binnen de organisatie onvoldoende kennis is over informatiebeveiliging en de BIO, dan wordt het een worsteling om hieraan goed invulling te geven. De afgelopen jaren kreeg ik steeds vaker de vraag om een trainingsprogramma te ontwikkelen specifiek over de BIG, BIR of andere baselines. Toen die werden samengevoegd naar de BIO zijn we direct gestart met de ontwikkeling van een programma dat overheidsbreed een vertaling maakt van de BIO naar de praktijk.

Training

Sinds 2020 is er een training en certificeringsprogramma voor de BIO genaamd Certified BIO Professional. De training vergroot de kennis van informatiebeveiliging en maakt je een betere gesprekspartner binnen de eigen organisatie maar ook naar andere overheidsorganisaties, partners en leveranciers. De training is een vertaling van de BIO naar de praktijk en is er op gericht om prestaties van medewerkers te verbeteren. Met deze BIO-examentraining kunnen organisaties aantoonbaar maken dat medewerkers kennis van de BIO hebben, wat weer bijdraagt aan BIO-compliance.

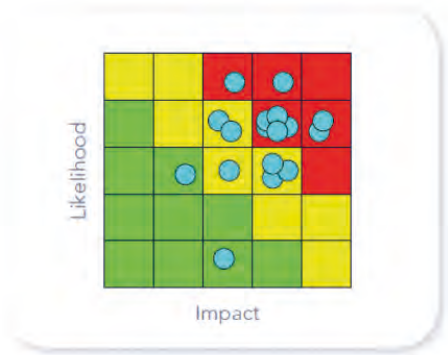
De baseline informatiebeveiliging voor de Nederlandse overheid heeft een grote meerwaarde. Doordat er één normenkader is, is er uniformering in de toepassing van informatiebeveiliging tussen ketenpartners. Als overheidsorganisatie weet je welke maatregelen in de basis van je worden verwacht en hoe je specifieke aanvullende maatregelen moet treffen. De eigen beveiligingsorganisatie kan gericht worden opgeleid en getraind. Er zijn ook allerlei handreikingen specifiek voor de BIO ontwikkeld die je in staat stellen er invulling aan te geven. Als je de BIO kunt toepassen en weet te interpreteren, dan is het wat mij betreft een geschenk.

Auteur: Robert Metsemakers schrijft op persoonlijke titel en is als ervaren IT-auditor en informatiebeveiligings-expert beschikbaar voor security-advies en (algemene) schrijfopdrachten via robert.metsemakers@gmail.com.

BLOG

Sinterklaas, verlanglijstjes en de security threat heatmap

In een verzonnen vergadering bespreken de deelnemers het gebruik van een heatmap met daarin een groot aantal security threats.



Figuur 1 – Example of soft-scoring heat map.

De roetveegpieten roezemoesten tijdens het wachten op de nieuwe Sinterklaas. In zijn eerste 100 dagen als directeur IT kwam hij één keer per afdeling naar het werkoverleg. Op dag 90 was de security-afdeling aan de beurt. Sinterklaas kwam binnen en zei: "Ik heb geen geschiedenis gestudeerd en ben ook niet van plan er nu mee te beginnen." Volgens Linkedin had hij wel Nederlands Recht gestudeerd en qua belangstelling en achtergrond leek hij meer gericht op verantwoordelijkheden en aansprakelijkheden dan op fijnmazige technische analyse. Nadenk-piet had een presentatie voorbereid met een analyse hoe de huidige probleemsituatie qua security ontstaan was. Dat stuk kon hij overslaan. De vergadertafel was vol. Een aantal pieten stond. Logging-piet zat op een archiefkast. "Nee, er zijn niet te weinig stoelen…" zei Sint dreigend. De toon was gezet toen hij onthulde dat je elke euro maar één keer kunt uitgeven. Meerdere pieten zagen hun 'management bullshit bingokaart' vollopen. Weldra zou de winnaar bekend zijn!

Nadenk-piet toonde een heatmap op het grote scherm. In het groen-oranje-rood gekleurde kwadrantenschema stonden 17 threats als genummerde bolletjes. "Wat is dat?," vroeg Sinterklaas. "Dat is de heatmap die we van u moesten overnemen van de Risk-afdeling, zodat de rapportages van onze afdelingen meer op elkaar zouden lijken," riposteerde Nadenk-piet eerlijk, maar onhandig. Sint wuifde korzelig, ga door, met zijn hand.
"We letten als security op beschikbaarheid, integriteit en vertrouwelijkheid en hebben voor alle drie theoretisch mogelijke bedreigingen gevonden. Die zijn aangevuld met hier opgetreden security incidenten die nog eens kunnen gebeuren. We overleggen regelmatig met branchegenoten over hun security incidenten. Daar hebben we er ook een paar van opgenomen. Het jaarlijkse dreigingsbeeld van NCSC heeft tevens aandacht voor internationale dreigingen. Eentje hebben we overgenomen. Van alle dreigingen heeft een expertgroep geschat wat de kans van een impact bij optreden is. Eerst bruto, dus als we niks zouden

"What's worse than doing nothing about risk management would be an organization luring itself into a false sense of security – and wasting resources – by using soft scoring or unproven methods and believing in them."

Douglas W. Hubbard

doen aan maatregelen. Veel dreigingen zijn extern en de kans hangt af van de intentie van de aanvaller. Daarna hebben we alle getroffen maatregelen opgeschreven en per stuk uitgebreid besproken of ze preventief, detectief of correctief zijn en tegen welke dreigingen ze werken. Daarmee zijn de netto kans en impact bepaald, die daarna zijn ingetekend op de heatmap. Rechtsboven staan de dreigingen die, na het nemen van alle maatregelen tot nu toe, nog steeds vaak kunnen gebeuren en dan een grote impact of schade zullen veroorzaken." Nadenk-piet zweeg. "Mooi verhaal, al is het mij wat te academisch. Ik hoef security dus alleen geld te geven voor de bolletjes rechtsboven?," vroeg Sinterklaas.

"Je hebt het niet begrepen" zei Nadenk-piet. Per definitie kan immers geen van de opstellers in de toekomst kijken: er zullen dus dreigingen vergeten zijn. Ook kunnen er dreigingen overbodig op de lijst staan omdat ze uiteindelijk slechts eens per 100 jaar optreden. Kans en impact zijn gebaseerd op subjectieve inschattingen. Weliswaar door deskundige experts, maar via een discussieproces tot een gezamenlijk compromis gebracht. De lijst met maatregelen kan incompleet zijn. Het effect van maatregelen kan te optimistisch ingeschat zijn, zodat de netto kans of impact te laag is berekend. Het benodigde budget is bovendien niet voor de afdeling security. Juist andere afdelingen moeten aan het werk, investeringen doen en eerder afgesproken acties eindelijk eens (volledig) uitvoeren. Dit dacht Nadenk-piet, maar hij zei het volgende:

"Het gaat over kansen. We schatten in dat deze threat hier linksboven slechts eens per jaar op zal treden. Maar dat kan wel morgen al zijn. En de threats rechtsonder zullen niet veel impact hebben, denken we, maar dat geldt alleen als alle genomen maatregelen op hetzelfde niveau blijven werken. En deze dreigingen treden zo vaak op dat alle individuele schades bij elkaar toch een behoorlijke impact hebben."

Sinterklaas zei dat hij verdorie Sinterklaas niet was. Daar keek men van op: dit stond niet op de bingokaart. Meteen ging hij toch in op verlanglijstjes. Kinderen stelden hem ieder jaar idiote vragen en hij gaf altijd alleen de eerste drie of vijf gevraagde cadeaus van het lijstje. Waarom kon dit bij security ook niet gewoon zo?

Nadenk-piet durfde niet meer te zeggen dat ook de threats met lage netto kans en impact linksonder niet compleet verwaarloosd konden worden. Bleek om de neus ging hij zitten. Geld-piet kwam hem te hulp. "Het is zoals kosten van schoolgaande kinderen. Die moeten eten, geld voor melk of thee op school, kleding, een fiets, schoolgeld, schoolboeken en een smartphone voor roosterwijzigingen via WhatsApp. Een hele waslijst, maar je kunt niet één van die zaken weglaten. En zelfs als je ze een extra mooie telefoon geeft, hebben ze toch nog een fiets nodig." Nadenk-piet knikte. Door implementeren van securitymaatregelen veranderen bruto-netto berekeningen en verschuiven de plaatsen van de dreigingen op de heatmap en daarmee de onderlinge prioriteit.

Hij vermande zich, stond op en sprak: "We moeten die hele heatmap wegdoen bij security. Het is een aardige grafiektechniek om een uitputtende lijst met de risico's van door externe auditors vastgestelde issues op te plotten. Maar het is ongeschikt om te kiezen aan welke security threats je de komende periode helemaal niets gaat doen." Terwijl hij de frisse buitenlucht in liep, dacht hij aan het citaat van Douglas W. Hubbard.

Douglas W. Hubbard
http://www.hubbardresearch.com/wp-content/uploads/2019/06/Broken-Risk-Management-Guide-Hubbard-Decision-Research.pdf

Auteur: Arash Rahmani is een digitaal strateeg gefocust op digitale transformatie met een nadruk op informatiebeveiliging. Met zijn expertise helpt hij organisaties als trusted advisor voor de CISO en andere leidinggevenden of als ad interim manager. Arash is bereikbaar via www.rahmani.nl.

Organisatiecultuur is essentieel voor informatiebeveiliging

Informatiebeveiliging is niet alleen een technische kwestie, maar ook een culturele. Een onderwerp dat begrip en steun nodig heeft op alle niveaus van de organisatie.

"Security transcends technology and culture eats strategy for breakfast"

– Peter Drucker Amerikaans schrijver, hoogleraar en consultant.

Enkele jaren na de Iraanse revolutie werd ik geboren terwijl het ziekenhuis werd gebombardeerd. Ik startte mijn leven in een omgeving vol chaos, continue onzekerheid en veranderingen. Directe familieleden verloor ik, omdat ze opkwamen voor democratie en vrijheid tijdens deze revolutie. Ze betaalden daar de ultieme prijs voor: langdurige marteling en uiteindelijk executie.

Van kinds af aan ben ik opgevoed met niet goedgelovig te zijn, de dingen die mensen zeggen te verifiëren, en er vanuit te gaan dat mensen andere agenda's kunnen hebben. Ik ben me bewust van hoe ik met informatie omga en ik weet dat niet iedereen in mijn leven toegang nodig heeft tot alle informatie. Ik kan omgaan met veranderingen en heb reserves en back-ups. Ik bouw altijd redundancy in en bereid mij voor op het ergste en hoop op het beste. Deze dingen zijn voor mij net zo natuurlijk als fietsen en je fiets goed op slot zetten dat zijn voor een kind dat opgroeide in Nederland.

Als kind hebben deze normen mij nooit belemmerd en ik heb er geen negatieve associaties bij. De normen hebben mij juist geholpen om vooruit te denken en stressbestendig te zijn. Als volwassene kwam ik erachter dat de dingen die onderdeel waren van mijn opvoeding, voor mij inmiddels natuurlijk zijn, essentieel zijn voor beveiliging en informatiebeveiliging. Ik was onbewust bekwaam op dit gebied en werd bewust van mijn bekwaamheid.

Inmiddels woon ik al jaren in Nederland, beschouw ik mijzelf als Nederlander en ben ik trots op ons kleine, vrije land dat groot is als het gaat om digitale infrastructuur en digitale innovatie. Ik ben een digitaal strateeg met de nadruk op informatiebeveiliging. Door de jaren heen heb ik bij verschillende nationale en internationale organisaties in de keuken mogen kijken en hen mogen helpen om hun digitale weerbaarheid te versterken door aandacht te besteden aan technologie, mensen, processen en cultuur.

Gemiste kans

Hoe meer ik bij organisaties binnen mocht kijken, hoe meer ik mij ervan bewust werd dat wat voor mij vanzelfsprekend is, niet of nauwelijks werd geïmplementeerd bij veel organisaties. Dit vormde vanzelfsprekend een risico voor de bedrijfscontinuïteit. In veel bedrijven is informatiebeveiliging niet in de cultuur verankerd, met het effect dat de volwassenheid met betrekking tot informatiebeveiliging zeer laag is. Directieleden zijn er niet mee bezig en reageren pas op het moment dat iets is gebeurd. Dan moet er snel een quick fix komen. Hoewel informatiebeveiliging niet van levensbelang is voor hen als persoon, is dat vaak wel het geval voor hun bedrijf en de continuïteit van hun bedrijf. Informatiebeveiliging is cruciaal voor een digitale transformatie en draait om veel meer dan technologie. U kunt de meest geavanceerde beveiligingstechnologie hebben, maar als er niet in de mensen, processen en cultuur wordt geïnvesteerd, zal informatiebeveiliging aanzienlijk minder effect hebben. Dat is mijns inziens een gemiste kans.

Een CISO moet de business begrijpen

Naar mijn mening kan een CISO meer waarde toevoegen aan een bedrijf als hij of zij het bedrijf begrijpt. De CISO heeft inzicht in de missie van de onderneming, haar doelstellingen en objectieven, strategie, cultuur, activa, het risicoprofiel,

Informatiebeveiliging is de verantwoordelijkheid van iedereen

de (wettelijke) nalevingsverplichtingen en de zakelijke trends. Een CISO moet in staat zijn om de business te helpen met het uittekenen van alle processen en deze te begrijpen. Een CISO moet communicatief sterk te zijn, commercieel kunnen denken, goed zijn in stakeholdermanagement en voldoende verstand hebben van marketing om gedragsverandering te kunnen realiseren en de organisatie mee te krijgen in de veranderingen. Een CISO dient bedreven te zijn in cybersecurity, IT, bedrijfsstrategie en het vermogen te hebben om mensen te leiden en aan zich te binden.
Als je vastzit in de IT-afdeling en je alleen richt op de IT-afdelingen, los je de bedrijfsproblemen niet op. Je moet de business inclusief haar mensen, processen en cultuur begrijpen. Je moet voortdurend gesprekken voeren met mensen van verschillende afdelingen om iedereen op één lijn te krijgen en om hun processen en uitdagingen te begrijpen, om ze zo mede-eigenaar te maken van het belang van informatiebeveiliging. Je moet de taal van de business kunnen spreken en verstaan. Pas dan kan je een effectieve informatiebeveiligingsbeleid opstellen en implementeren. Wat ik vaak tegenkom is dat zowel vanuit de externe consultant, de CISO net zoals de business de gedachte leeft dat informatiebeveiliging een IT-probleem is en dus ook een IT-oplossing nodig heeft. Er wordt veel geïnvesteerd in technologie, iets wat waardevol is, maar er word onvoldoende geïnvesteerd in mensen, cultuur, gedragsverandering, processen in kaart brengen en elke stap beveiligen. Het is een illusie om te denken dat awareness een synoniem is van gedragsverandering.

Volwassen informatiebeveiliging

De wereld verandert continue. Ondanks dat de meeste veranderingen langzaam gaan, ervaren veel mensen die veranderingen als stressvol en snel. Verandering is een kans op vooruitgang en organisaties ontkomen er niet aan dat ze moeten veranderen en innoveren. De grote witte haai moet constant blijven zwemmen om zijn zuurstoftoevoer via de kieuwen op peil te houden, anders is er kans dat het dier komt te overlijden. Hetzelfde principe geldt voor bedrijven, zij moeten in beweging blijven, zich aanpassen aan de veranderende wereld om hen heen en moeten in staat zijn de risico's die met de verandering gepaard gaan te beheersen. Informatiebeveiliging houdt niet op, het is niet iets dat je eenmalig doet, het moet deel uitmaken van de mentaliteit, van elk proces binnen een bedrijf en de cultuur. Succesvolle digitale transformaties, waar informatiebeveiliging verankerd is, gaan gepaard met een cultuur die de noodzaak en de risico’s van informatiebeveiliging begrijpt en openstaat voor ideeën, verandering, verbeteringen, om van fouten te leren en die mensen beloont die waarde toevoegen. Niet met een cultuur die fouten belachelijk maakt en bestraft, een cultuur die in silo's werkt en mensen vertelt dat ze zich met hun eigen zaken moeten bemoeien. Het is van cruciaal belang dat mensen in staat zijn te herkennen wanneer zich een beveiligingsincident voordoet en dat er een cultuur heerst waarin mensen zich op hun gemak voelen om een incident te melden of een verbetering voor te stellen. Informatiebeveiliging is de verantwoordelijkheid van iedereen. Een taak van de consultant is om te helpen een cultuur te creëren waar ruimte is om de volwassenheid van informatiebeveiliging te verhogen.

Nieuwsgierig naar hoe je zo een cultuur kunt creëren en hoe je mensen van alle lagen van de organisatie kan meekrijgen om informatiebeveiliging te integreren in hun mindset? In toekomstige artikelen ga ik hier meer aandacht aan besteden en uiteraard kun je contact met mij opnemen voor een (virtueel) kopje koffie.

Auteur: Renco Schoemaker is senior adviseur informatiebeveiliging & privacy en mede-eigenaar bij IB&P. Momenteel is hij werkzaam bij een G4 gemeente als security officer en coördineert hij de ENSIA verantwoording. Eerder was hij adviseur en CISO (a.i.) bij diverse gemeenten. Renco is bereikbaar via r.schoemaker@ib-p.nl.

Met de BIO bezig blijven: hoe lang?

Met de Baseline Informatiebeveiliging Overheid (BIO) ben je nog wel even bezig. Net zoals je daarvoor al de nodige jaren besteedde aan haar voorlopers, zoals de Baseline Informatiebeveiliging Gemeenten. Cynisch bezien kun je stellen dat je jaren bezig bent met de implementatie, mits het normenkader steeds maar wijzigt. Oude wijn in nieuwe zakken is ons niet vreemd. Vandaag echter geen rauw cynisme, maar een oprechte poging te ontleden waarom dat 'vaart maken' voor gemeenten zo verrekte lastig is.

Het is geen willekeur dat ik met dit onderwerp begin. Tot mijn verbazing zijn we er maar mondjesmaat in geslaagd het management dermate te overtuigen dat zij intrinsiek gemotiveerd is geraakt om tijd en middelen te steken in informatiebeveiliging. Je kent hun immer relativerende uitspraken vast wel uit je eigen praktijk. Het belang van informatiebeveiliging mag inmiddels duidelijk zijn toch, denk je dan. Gezien de gedwongen winkelnering bij de overheid moet het juist daar op orde zijn! Het angstargument volstaat echter niet. Het voorbeeldgedrag valt dus tegen en dit dienen we onszelf grotendeels aan te rekenen: een onvoldoende voor business alignment, wat mij betreft. En dat schaadt ons vak, want goed voorbeeld doet goed volgen.

Op bestuurlijk niveau loopt het ook niet echt storm. We blijven steken bij tien goedbedoelde principes en een krappe voldoende voor het inrichten van intern (horizontaal) toezicht door de gemeenteraad. Áls de raad al geïnformeerd wordt. En grasduin eens door een aantal rekenkamerrapporten, je zult ontdekken dat we het daarmee ook niet gaan redden: te algemene en wollige aanbevelingen in termen als PDCA, ISMS en GRC. Maar vooral: nauwelijks follow-up! Op een enkele pijnlijke kwetsbaarheid die uit een pentest rolt, na.

Veiligheidscultuur

Managers en bestuurders die voor de troepen uitlopen zijn essentieel voor de sterkte van de veiligheidscultuur binnen een organisatie. Kai Roer onderscheidt in zijn werk in totaal zeven dimensies van een sterke veiligheidscultuur. Zonder het ontstaan van een dergelijke cultuur blijven bewustwordingscampagnes grotendeels mislukken of op z'n best alleen op korte termijn werken. En nee, het is naïef zwaar te willen leunen op de integriteit van mensen als escape.

Als CISO ga je deze cultuur niet in je eentje vormgeven. Daar heb je de tijd niet voor en zeer waarschijnlijk ook de kennis niet. En nog belangrijker: die positie heb je gewoonweg niet. Dat is niet erg, maar het is goed je bewust te zijn van je bescheiden invloed op de veiligheidscultuur. Al je goede initiatieven ten spijt. Dat jij enthousiast bent en het belangrijk vindt verwacht iedereen; het is immers je werk zogezegd. Het zijn de managers en bestuurders die voorop moeten omdat hun voorbeeldgedrag nu eenmaal veel meer impact heeft dan het jouwe.

Het CISO-schaap

Over de CISO gesproken, die moet werkelijk van alles kunnen. En meestal daarbij accepteren dat hij/zij minstens één schaal te laag is ingeschaald en ofwel geen fulltime dienstverband heeft, ofwel de CISO-'rol' mag combineren met iets anders. Als CISO moet je goed overweg kunnen met de veelheid aan instrumenten, formats en templates die beschikbaar zijn vanuit het gemeentelijke CERT (IBD). Ook is het prettig als het goed botert met de privacy collega's zoals de functionaris gegevensbescherming en de privacy officer.

Helderheid over wie wat doet en mag is wenselijk. Bedrijfscontinuïteitsbeheer ligt meestal ook op je bord. Bofkont. En had ik al gezegd dat je actuele kennis moet hebben over relevante wet- en regelgeving, normenkaders, frameworks en zo? Vergeet niet het management en het bestuur mee te nemen, dat 30 urgentere onderwerpen te bespreken heeft. En de Plan-Do-Check-Act-cyclus op te zetten. Incidenten hebben voorrang op alles. You get the picture. Ben jij dat niet-bestaande schaap met de vijf poten?

Kortzichtig over ISO27001

Ten tijde van de BIG is er door veel CISO's – de ingehuurde incluis – veel te licht gedacht over het managementsysteem voor informatiebeveiliging. Ook wel het Information Security Management System, wat lekkerder bekt als ISMS. ISMS is de

De B in BIO staat niet voor Bezig of Blijven

Plan-Do-Check-Act-cyclus ingevuld voor informatiebeveiliging en is derhalve het proces waarbinnen beveiligingsmaatregelen worden genomen. Daar is heel veel óver gepraat door de jaren heen, maar er zijn maar bar weinig gemeenten die een goed werkend ISMS-proces hebben, hoe bescheiden ook. Buiten de (lokale) overheid om praten we trouwens gewoon over de ISO27001 norm voor het ISMS met op het gebied van privacy de jongste telg: ISO 27701. En de BIO is in tegenstelling tot de BIG gelukkig wel een één-op-één doorvertaling van de ISO27002, ook wel de implementatierichtlijn genoemd.
Er is door menig gemeente veel te snel ISMS-software ingezet in de hoop en verwachting dat daarmee het PDCA proces gaandeweg wel zou gaan lopen. Niets bleek minder waar. Bedenk dus goed wanneer en hoe je ISMS-software inzet. Ander punt van aandacht is het op poten zetten van risicomanagement op het gebied van informatiebeveiliging, samen met het lijnmanagement. Of, wanneer je geluk hebt, risicomanagement in z'n geheel. De BIO lijkt hierbij te hinken op twee gedachten: enerzijds risicomanagement bedrijven met behulp van het ISMS (27001) en anderzijds een basisbeveiligingsniveau afdwingen via de implementatierichtlijn (27002).

Nadruk op ISO27002

Voor dat laatste moeten we de Rijksoverheid bedanken. Die wilde wel erg graag dat de overgang van de BIR – waarvan de inkt in 2017 nog nat was – beleidsneutraal zou zijn. En dus hangt het ISO27001 deel er wat ongelukkig bij. Enfin, in de BIG kreeg het praktisch nul aandacht dus dat is alsnog winst. Nu staat wat mij betreft de nut en noodzaak van baselines niet ter discussie. Toch is en blijft het lastig om vanuit het managen van maatregelen 'op te klimmen' naar het managen van risico's. Terwijl het wel daar om draait, nietwaar? Anders ga je die managers en bestuurders zeker niet aanspreken en verwordt informatiebeveiliging tot een plichtmatig af te werken vinkenlijst. Wat dan ook niet helpt is de van oudsher aanwezige nadruk op het naleven van wet- en regelgeving. Ofwel, de nadruk op compliance. Met de komst van de Eenduidige Normatiek Single Information Audit (ENSIA) is de auditlast – gericht op de naleving van normenkaders – enigszins gedaald, maar ik durf toch te stellen dat ENSIA slechts minimaal wordt benut. ENSIA kan zoveel meer zijn dan de (beperkte) C in de PDCA-cyclus. Van mijn eerder in het iB-Magazine beschreven toekomstscenario's voor ENSIA, komt vooralsnog weinig terecht.

Dus: bezig blijven

De B in BIO staat niet voor Bezig of Blijven, maar ik denk wel dat de implementatie ervan bij veel gemeenten een lang verhaal wordt (is). Uitgezonderd een enkele (grote) gemeente, hoor ik in gemeenteland niets over een ISO27001-certificering, terwijl de provincies daar al in 2018 toe besloten. Daarmee worden, zo vrees ik, teveel (losse) BIO-maatregelen (ad-hoc) genomen. Veel Plan en Do, maar nauwelijks via Check en Act terug naar Plan. En daarmee poetsen we die onvoldoende op business alignment niet weg. Hopelijk heeft dit artikel je een overzicht gegeven in mogelijk oorzaken van het stroperige tempo op de BIO-implementatie. En ik hoop dat het je helpt je schaarse tijd goed te besteden. Ofwel: blijf inderdaad nog jaren bezig met die BIO, maar dan wél op zo'n manier dat het ieder jaar meetbaar een stukje beter gaat en dat het stuur ieder jaar een beetje meer overgaat naar het management. Bouw aan het (management)systeem!
Ik heb meer blogs geschreven over de genoemde onderwerpen, voor de liefhebber zijn deze terug te lezen op de website van IB&P (1).

Referentie

((1) Het overzicht met 25 verwijzingen naar eerdere blogs vind je op https://link.ib-p.nl/verwijzingen (wachtwoord = pvib)

Auteur: Mark Tissink – Eigenaar van Secure IT is auteur van het boek 'Grip op informatiebeveiliging - Groei in leiderschap', trainer, spreker en coach. Door IT en Neurolinguïstisch Programmeren te combineren kun je anders kijken naar hetzelfde. Mark is bereikbaar via info@marktissink.nl.

In deze blogreeks neem ik je mee op reis om de wereld rondom informatiebeveiliging te bekijken vanuit mijn ogen. Naast audit zijn deze ogen ook getraind te kijken vanuit persoonlijke ontwikkeling en communicatie.

BLOGREEKS DEEL 1

Anders kijken... naar informatiebeveiliging

Nationale veiligheidsdiensten lijken in hun werk bij het maken van dreigingsanalyses op security-afdelingen. Uit hun praktijkervaring kunnen securityprofessionals daarom nuttige zaken leren.

Het begint namelijk niet bij de techniek maar bij de bovenkant van de organisatie: de directie, Raad van Bestuur (RvB) of board. Zij staan bovenaan en voeren de leiding over de betreffende organisatie. Deze 'tone at the top' of 'demonstrate leadership' is ontzettend belangrijk. Maar hoe kan leiderschap getoond worden voor informatiebeveiliging? Heel simpel: als informatiebeveiliging door hen niet belangrijk gevonden wordt, krijgt het ook geen aandacht en gaat het niet gebeuren! Informatiebeveiliging begint met het maken van keuzes. Deze keuzes zullen vervolgens verankerd moeten worden in een strategisch beleid en er zullen rollen en (eind)verantwoordelijkheden moeten worden toegekend. De board moet dat regelen, of ervoor zorgen dat er mensen zijn die dat voor hen gaan regelen. Bij kleinere organisaties zal de directie zelf een actievere betrokkenheid hebben. En wanneer de organisatie groter wordt, moeten zij zorgen voor de juiste governance, het besturen. Daarbij moet een framework voor de beheersing juist ingericht worden, zodat zij de juiste signalen krijgen op de juiste momenten.

Zij moeten in staat gesteld worden om de juiste keuze te maken, door ervoor te zorgen dat op het juiste moment de benodigde informatie aanwezig is. Dit kan weer leiden tot de juiste opvolging.

Leef je in

Wat vragen we dan concreet van de directie? Uitdragen van datgeen wat belangrijk gevonden wordt. Hoeveel focus op dikke omzet draaien en hoeveel focus op degelijke kwalitatieve bedrijfsvoering? Deze twee hoeven elkaar niet uit te sluiten, maar helaas is mijn ervaring dat dit vaak wel zo wordt gezien. Vervolgens is het van belang dat juist op dit strategische niveau een koppeling gelegd wordt naar de missie en visie van het bedrijf. De why (1) moet vertaald worden naar het belang van het wel of niet hebben van bepaalde kwaliteitsstandaarden. En dit bedoel ik niet primair vanuit de wetten en regels, maar vanuit de intrinsieke motivatie. Waarbij het gaat om 'het goed doen', ook zonder dat daar een stok of een wortel tegenover staat. Daarna is het een kwestie van uitdagen 'hoe' dit dan gedaan kan worden. Wat is de exacte vraag aan de individuele medewerker? Door het zo toegepast mogelijk, op concrete werksituaties, te blijven communiceren zal na verloop van tijd een nieuwe manier van werken ontstaan. En sta open voor het commentaar en de opmerkingen die medewerkers geven. Het feit dat ze reageren betekent dat er een wens is tot betrokkenheid! Kijk wat er eventueel extra nodig is of geef, wanneer dat niet mogelijk is duidelijk uitleg over duidelijk uitleg over. "Probeer hen eerst te begrijpen voordat het jouw recht wordt om begrepen te worden. Leef je in de werksituatie van deze medewerkers in." Het bewust inrichten van een cultuur en vervolgens daarop blijven sturen, is één van de lastigste elementen die een organisatie kan proberen te beheersen. Dat is namelijk niet zomaar in een middag gedaan. Afhankelijk van de omvang van de organisatie, is dit een proces van één of enkele jaren. Uiteindelijk zal dit over de loop van maanden of jaren, afhankelijk van de grootte van de organisatie, leiden tot een cultuuromslag. Daarmee hebben we de nieuwe manier van werken gecreëerd. Ook het alloceren van voldoende mensen en middelen om gedaan te krijgen wat er moet gebeuren is belangrijk. We kunnen wel zeer goede informatiebeveiliging willen, maar als er maar anderhalve man en een paardenkop voor verantwoordelijk is, zal dit niet gaan werken.

Voorbeeld van transparantie: Universiteit Maastricht

Een goed voorbeeld van deze transparantie is de Universiteit van Maastricht (3). Er is online een 47 pagina's tellende rapportage beschikbaar over de werkwijze en afhandeling van de ransomware die zij ruim een jaar geleden over hun organisatie heen kregen. Hierin staat ook beschreven hoe door het College van Bestuur de (risico)afweging gemaakt is over de keuze om wel of niet het losgeld te betalen. Aanvullend gaat het ook over de tekortkomingen en de daaropvolgende acties. Deze manier van handelen draagt enorm bij aan de algehele digitale weerbaarheid van Nederland.

Transparantie van gedrag

Tot slot wil ik het nog hebben over de transparantie van gedrag. Een aspect dat ook naar voren komt bij de acht basissoftcontrols (2). Hoe beter organisaties hun eigen handelen kunnen waarnemen, introspectie, inclusief het effect ervan, hoe beter ze in staat zijn om het eigen gedrag aan te passen aan de verwachtingen van anderen. Op bestuursniveau kan dit ook betekenen dat daar waar te kort geschoten wordt bijvoorbeeld in de informatiebeveiliging, dat ook hierover gesproken en/of gerapporteerd wordt. Er is openheid over geslaagde en niet-geslaagde hackpogingen. Net als openheid over datalekken en risicoanalyses. Beseffen en communiceren dat het niet is zoals je wilt en daar actie op ondernemen. Door deze transparantie ontstaat ook een welwillendheid tot verbetering en tot groei.

Geen compromissen

De informatiebeveiliger mag nooit de beslisser zijn, maar zit in een controlerende en vervolgens adviserende rol. Wanneer de directie het advies onvoldoende opvolgt, kunnen we niets anders dan wijzen op de risico's en – voor ons het belangrijkste – CYA, Cover Your Ass. Mocht het zo uit de hand lopen en hard indruisen tegen je morele en ethische kompas, dan zal er verdere escalatie nodig zijn. In het ergste geval kan dit in de vorm van een officiële klokkenluidersrol. Maar laten wij het zover komen? Ik vind dat wij als informatiebeveiligers sneller moeten besluiten en eieren voor ons geld moeten kiezen wanneer een organisatie het niet al te nauw neemt met het volgen van de regels. Voor goede mensen is altijd plek. Ga staan voor wat jij belangrijk vindt. Geen compromissen. En ook dát is leiderschap… persoonlijk leiderschap.

Delen van dit artikel zijn overgenomen uit mijn boek.

Referenties

(1) Simon Sinek – Start with Why

(2) Muel Kaptein – Acht basis softcontrols

(3) https://www.maastrichtuniversity.nl/um-cyber-attack-symposium-lessons-learnt

In deze rubriek geven enkele iB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over informatiebeveiliging. Dit zijn persoonlijke reacties van de auteurs en deze geven niet noodzakelijkerwijs het officiële standpunt weer van hun werkgever of van PvIB. Vragen en/of opmerkingen kun je sturen naar ibmagazine@pvib.nl.

Wat maakt het BSN-nummer zo bijzonder?

'Wees extra alert' kopte de NOS nadat bleek dat gegevens uit het coronasysteem eenvoudig door heel veel (tijdelijke) GGD-medewerkers geëxporteerd konden worden. Niet in de laatste plaats omdat dit systeem het BSN verwerkt. Zelfs DUO haalde het nieuws toen er per abuis 1700 BSN's zichtbaar waren achter het envelopvenster. Wat is het toch dat het BSN zo bijzonder maakt? En hoort dit nummer eigenlijk wel zo bijzonder te zijn

Stop met 'geheime' vragen! – Maarten Hartsuijker

Een BSN-nummer hoort natuurlijk geen waarde te hebben. Het nummer is enkel een koppelgegeven, bedoeld om mijn persoonsgegevens in administraties te kunnen terugvinden en om ze over administraties heen met elkaar te kunnen verbinden. Vanuit dat perspectief is het dus geen enkel probleem als anderen jouw BSN kennen. Het zijn de gegevens die eraan gekoppeld zijn die écht vertrouwelijk zijn. Tot zover de theorie. Maar de praktijk is volkomen anders. Organisaties die de aan jouw BSN gekoppelde gegevens moeten beschermen, worstelen namelijk met het authentiseren van hun klanten: de burgers, verzekerden, studenten. Je zou denken: daarvoor hebben we inmiddels DigiD. En dat klopt, daar waar het digitale kanaal betreft. Maar bij elk niet gedigitaliseerd proces moeten bellers en mailers zich op een andere manier identificeren en authentiseren, en daar gaat het mis. Organisaties vallen in deze processen massaal terug op het stellen van vragen als: wat is uw geboortedatum, rekeningnummer, BSN, postcode, huisnummer, geboorteplaats ... Terwijl iedereen eigenlijk wel weet: de antwoorden daarop waren al nooit echt een geheim, maar zijn dat door het gebruik van social media en de continue stroom aan datalekken tegenwoordig zeker niet meer. Stop dus met 'geheime' vragen! Stop met het zien van het BSN als een geheim en maak het niet waardevoller dan het is!

BSN als attribuut van een identiteit – Tom Bakker

Wat opvalt bij het GGD-lek is dat het een insiders threat incident was. Dit risico blijft toch een niet te onderschatten dreiging. Het is dan ook een vaker voorkomend incident. Dit risico kan zich manifesteren door infiltratie van criminelen of (tijdelijke) medewerkers die toevallig mogelijkheden zien (de gelegenheid maakt de dief). Zie ook het Verizon 2020 Data Breach Investigations Report (1). Juist in de zorg is de verdeling van threat actors in- en extern fiftyfifty. Preventie (VOG, screening, IAM) en monitoring zijn hierbij belangrijk. Dan zijn er ook nog de domme fouten, zoals bij DUO.

Een lek waarbij het BSN 'op straat' ligt, zou minder impact hebben wanneer het BSN niet zo bijzonder zou zijn. Met andere woorden: je zou met alleen het BSN niet zo makkelijk misbruik kunnen maken. Omdat het BSN zo bijzonder is, moet het geheim blijven. Aan de ene kant wordt met kunst en vliegwerk gepoogd het BSN geheim te houden binnen allerlei toepassingen. Denk aan versleuteling en het toepassen van 'polymorfe pseudoniemen' (2) om het BSN af te schermen. Aan de andere kant was een tijdlang het BSN onderdeel van het btw-nummer van ZZP'ers. Het btw-nummer vermelden was verplicht op hun facturen. Hoezo geheim? Inmiddels is dit 'lek' door de overheid aangepakt door uitgifte van nieuwe btw-nummers, zonder BSN. De oplossing: beschouw het BSN gewoon als attribuut van een identiteit. Met de afzonderlijke persoonsgegevens kun je niet zo veel uitrichten.

Bewustwording van de risico's – Bianca Brooijmans

Het BSN is een uniek persoonsgebonden nummer in Nederland, dat bij geboorte wordt uitgegeven en de rest van je leven (en daarna) jouw persoonlijke nummer blijft. Volgens de rijksoverheid is het BSN een 'informatieloos' nummer, waar geen persoonlijke informatie, zoals een geboortedatum, in is verwerkt. Je zou een persoon daarom niet kunnen herkennen aan een BSN. Met het enkele gegeven van het BSN klopt dat wellicht, echter juist dat unieke nummer gebruikt de overheid om persoonsgegevens te verwerken en overheidszaken te regelen. Variërend van uitkeringen tot identiteitsbewijzen. Kortom, het BSN is een van de belangrijkste gegevens ter identificatie van burgers en in de administratie van de overheid.

Onder de Wbp (Wet bescherming persoonsgegevens), de voorloper van de AVG, was het BSN in artikel 24 wel opgenomen als bijzonder persoonsgegeven, in de AVG niet meer. Bijzonder, omdat artikel 9 AVG een aantal bijzondere persoonsgegevens wel specifiek benoemt en hier in overweging 51 bij stelt: 'Persoonsgegevens die door hun aard bijzonder gevoelig zijn wat de grondrechten en fundamentele vrijheden betreft, verdienen specifieke bescherming aangezien de context van de verwerking ervan significante risico's kan meebrengen voor de grondrechten en de fundamentele vrijheden.'

Artikel 87 AVG biedt de lidstaten wel de mogelijkheid om specifieke voorwaarden en maatregelen te treffen voor het gebruik en de verwerking van een persoonlijk identificatienummer (zoals het BSN). Nederland heeft dit artikel concreet vormgegeven in artikel 46 UAVG – Verwerking nationaal identificatienummer. We kunnen dus stellen dat Nederland het BSN terecht behandelt als ware het een bijzonder gegeven met risico's voor het individu en zijn of haar persoonlijke levenssfeer. Misschien nog wel met een sterkere afscherming dan de categorieën als genoemd in artikel 9 AVG. Waar bijzondere persoonsgegevens in de AVG alleen met beperkte uitzonderingen gebruikt mogen worden, is het BSN voorbehouden aan overheid, zorg, onderwijs en in een

Het BSN is een vingerafdruk waarmee de relatie met de overheid geregeld wordt

zeer beperkte mate aan andere private partijen. En daar waar één van de uitzonderingen - zoals genoemd in de AVG - de toestemming van de betrokkene vereist, mag het BSN buiten deze sectoren zelfs niet mét toestemming worden verwerkt. Dat het nummer bijzonder hoort te zijn, lijkt me zonder twijfel een juist uitgangspunt. Nu wordt het tijd om meer bewustwording te creëren ten aanzien van welke wettelijke bepalingen grondslag bieden voor gebruik en de daadwerkelijke risico's die dit gebruik met zich meebrengt.

We moeten meer naar Multi-factor Authenticatie (MFA) – Fook Hwa Tan

We zien steeds meer lekken van inloggegevens. Naast het feit dat veel mensen hetzelfde wachtwoord gebruiken voor meerdere diensten, is gebruikersnaam en wachtwoord vaak makkelijk te raden. We zien in relatie tot de overheid, dat ons BSN-nummer vaak voldoende is om onszelf te identificeren en dat maakt het erg kwetsbaar. Daarom is het verstandig meer in meerdere factoren van authenticatie te denken.
MFA zorgt voor sterkere authenticatie, omdat je niet alleen iets moet weten (wachtwoord), maar ook moet hebben (apparaat, token) of moet zijn (biometrie). We zien dit ook steeds vaker als best practice, dat minimaal twee factoren worden ingezet voor authenticatie. Dit is echter niet voor alles het geval. Er wordt nog veel vertrouwd op een enkel wachtwoord. Wat tegenwoordig ook nieuw is, is dat je zelfs op basis van je locatie of gebruikte apparaat verschillende autorisaties kan krijgen. Systemen worden dus contextbewust. Er zal een verschil ontstaan waar je toegang toe hebt of je op kantoor zit of dat je vanuit huis werkt. Systemen kunnen ook detecteren of je bedrijfsapparatuur gebruikt of een eigen apparaat. Verder zien we ook, dat door nieuwe technologieën authenticatieprocessen veel gebruikers-vriendelijker worden gemaakt door het voor gebruikers makkelijker te maken om te authentiseren. Denk hierbij aan wachtwoordmanagers om complexe wachtwoorden in te vullen en apparaten waarbij je met een druk op de knop gebruik kan maken van je tweede factor, irisscan of vingerafdruk. Het is daarom nu tijd om met de technologie mee te gaan en niet alleen meer op één nummer (BSN) te vertrouwen als authenticatie middel, maar voor meerdere factoren te gaan. Vooral in de interactie met de overheid zou dit veel sneller doorgevoerd moeten worden, omdat we daar vaak direct invloed op onze levenssfeer kunnen uitvoeren.

Terecht bijzonder – Chris de Vries

Onze Rijksoverheid stelt: 'Het Burgerservicenummer is uw eigen persoonsnummer voor contact met de overheid. Bijvoorbeeld voor zorg of belastingen. U krijgt een BSN als u zich inschrijft in de Basisregistratie Personen (BRP)' (3). Het is terugvindbaar op paspoort, rijbewijs en identiteitskaart. Om identiteitsfraude tegen te gaan plaatst de overheid het BSN op minder zichtbare plaatsen. De geldigheid ervan is onbeperkt, hetgeen betekent dat zelfs de dood het BSN niet doet tenietgaan, het BSN is voor 'de eeuwigheid'! Dit is geregeld in de Wet algemene bepalingen Burgerservice-nummer (4). Hier wordt het gebruik van het BSN toegelicht te weten dat 'overheidsorganen het gebruiken bij het kunnen verwerken van persoonsgegevens in het kader van de uitvoering van hun taak, tenzij er sprake is van bijzondere omstandigheden.'

Wij constateren dat het BSN een vingerafdruk is waarmee de relatie met de boven ons gestelde overheid geregeld wordt. Verder weten wij dat nagenoeg alle overheden in geval van conflicten met de burger de bewijslast omdraait en dat de burger schuldig is tenzij … Wij leven 'eeuwig' voort in ons BSN, het stelt zonder enige twijfel vast dat de burger zelf een bepaalde handeling heeft verricht met de overheid en de consequenties daarvan heeft te dragen (getuige zijn BSN vaststelling tijdens die handeling). Nieuwe vraag: "Wat nu als ons BSN gestolen wordt (natuurlijk onmogelijk in ons uiterst secure overheid 's informatiebeveiligingsomgeving (?!), want DUO, GGD zijn slechts incidenten)? Ik denk dat het BSN inderdaad terecht bijzonder is en dat ook behoort te zijn!

Referenties

(1) https://enterprise.verizon.com/resources/reports/dbir/
(2) https://www.pvib.nl/actueel/ib-magazines/16-2
(3) https://www.rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens/vraag-en-antwoord/wat-is-het- burgerservicenummer-bsn
(4) https://wetten.overheid.nl/BWBR0022428/2018-07-28, hoofdstuk 4, paragraaf 1, artikelen 10 en 11

COLOFON

IB is het huisorgaan van het Platform voor InformatieBeveiliging (PvIB) en bevat ontwikkelingen en achtergronden over onderwerpen op het gebied van informatiebeveiliging.

PvIB
Platform voor InformatieBeveiliging

HOOFDREDACTEUR
Nicole van Deursen

REDACTIE
Tom Bakker
Bianca Brooijmans
Maarten Hartsuijker
Lilian Knippenberg
Rachel Marbus
Fook Hwa Tan
Chris de Vries

BLADMANAGEMENT
MOS bv
Caroline Knobbe
Sam Dekkers
E ibmagazine@pvib.nl

ADVERTENTIE-ACQUISITIE
MOS bv
E acquisitie@mos-net.nl
T 033 247 34 00

VORMGEVING
Neverseen Art & Design
Dimitri van den Berg

DRUK
VDR druk & print

UITGEVER
Platform voor Informatiebeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
T (033) 247 34 92
E secretariaat@pvib.nl
W www.pvib.nl

ABONNEMENTEN
De abonnementsprijs in 2021 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

ABONNEMENTENADMINISTRATIE
Platform voor Informatiebeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
E secretariaat@pvib.nl

ISSN 1569-1063

TSTC

ICT en Security Trainingen

ADVANCE YOUR CAREER WITH SECURITY IN 2021

CSA - Certified SOC Analyst
GSEC - Giac Security Essentials
GPEN - Giac Penetration Tester
EDRP - Disaster Recovery Professional
EHF - Ethical Hacking Foundation
CND - Certified Network Defender v2
CEH - Certified Ethical Hacker v11
CPENT - Certified Penetration Testing Professional

Want security start bij mensen!!

TECHNICAL SECURITY TRAININGEN

CEH - Certified Ethical Hacker
CHFI - Computer Hacking Forensic Investigator
CPENT - Certified Penetration Testing Professional
SSCP - Systems Security Certified Professional
OSCP - Offensive Security Certified Professional

SECURITY MANAGEMENT TRAININGEN

CISSP - Certified Information Systems Security Professional
CISM - Certified Information Security Manager
CISA - Certified Information Systems Auditor
CRISC - Certified In Risk And Information Systems Control
C|CISO - Certified Chief Information Security Officer

PRIVACY TRAININGEN

CIPP/E - Certified Information Privacy Professional / Europe
CIPM - Certified Information Privacy Manager
CIPT - Certified Information Privacy Technologist
CDPO - Certified Data Protection Officer

CLOUD SECURITY TRAININGEN

CCSP - Certified Cloud Security Professional

ISO TRAININGEN

ISO 27001 - Foundation
ISO 27001 - Lead Implementer
ISO 27001 - Lead Auditor
ISO 27005 - Risk Manager
ISO 27701 – Privacy Management

www.tstc.nl

Onze trainingen zijn weer klassikaal of Live Online te volgen