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.

Wanneer ben je open & transparant?

Goed nieuws: de medewerkers van de Autoriteit Persoonsgegevens (AP) maken zelf ook wel eens een foutje en ze zijn daar open over in hun jaarverslag (1). In totaal kreeg de AP met vijftig beveiligingsincidenten te maken, waarvan 26 datalekken. Die laatste gevallen gingen vooral om het verkeerd adresseren van brieven en e-mails. Ook ketenrisico's zijn de AP niet vreemd: de leverancier van een website had third-party plug-ins op de website geplaatst die gegevens doorstuurde naar Google. En niet alleen onze eigen AP maakt wel eens een foutje, ook het Britse National Cyber Security Centre (NCSC) moest haar bewustzijnscampagne intrekken omdat ze voor de campagne dezelfde naam had gekozen als de naam van een illegale streaming-app (2). Wellicht verschijnt dit incident ook in het jaarverslag.

We zijn meer bezig met incidenten en ook de openheid erover groeit. Inmiddels kijken veel mensen al niet meer op van berichten over ransomware, grote datalekken en kritieke kwetsbaarheden. Dat dit in het jaarverslag wordt opgenomen is een nieuwe stap in deze openheid. Hoe bewaken we de balans tussen openheid en transparantie aan de ene kant en het toch nog veel gehoorde statement 'aanvallers niet wijzer maken' aan de andere kant? Wat is maximale transparantie? Hadden we de beveiligingsincidenten bij de AP niet liever eerder willen weten? Een blik op deze materie van onze redacteuren.

Leo van Koppen - 'Een aanmoediging voor organisaties'

Deze openheid van het AP oogt natuurlijk heel eerlijk en ik keur het ook zeker niet af, maar ik vind het ook wel een beetje symboolpolitiek. De openheid beoogt volgens mij veel meer dan alleen het formele karakter van het melden van belangrijke wapenfeiten in een jaarverslag. Er wordt ook invulling gegeven aan de voorbeeldfunctie; een aanmoediging voor organisaties om ook deze openheid te betrachten in een paragraaf 'Beveiligingsincidenten'.

Daarnaast is het blijkbaar ook een goed PR-item want met een dergelijke vermelding kom je in het nieuws. Sommige organisaties heiligen het credo 'any news is good news', dat credo gaat hier blijkbaar ook op.

Formeel is de taak van het AP toezicht houden op het verwerken van persoonsgegevens. De Autoriteit Persoonsgegevens heeft als wettelijke taak te beoordelen of personen en organisaties de Wet bescherming persoonsgegevens naleven. Deze taak is ook gericht op de overheid. Ook ziet de AP toe op naleving van de Wet politiegegevens, de Wet gemeentelijke basisadministratie persoonsgegevens en alle andere wettelijke regelingen waarin sprake is van het verwerken van persoonsgegevens (3).

Leo van Koppen | Chris de Vries | Fook Hwa Tan | Lilian Knippenberg

Een blik op de website van de AP leert mij dat naast het controleren er ook veel aandacht besteed wordt aan voorlichting over relevante (nieuwe) wetgeving waaronder heel veel aandacht voor en best practices als het gaat om de AVG en dat is heel logisch. Ik vraag me overigens wel af of de invulling van die taak niet te veel is doorgeslagen naar het preventieve. Organisaties kennis aanreiken en daarmee naar verwachting het aantal datalekken terugdringen. Niets mis mee, want we doen niets anders in ons vakgebied. In onze preventieve strategie passen we de voorbeeldfunctie voortdurend toe, toch? In de awareness aanpak beleggen we de voorbeeldfunctie bij de CEO. Hij of zij moet het voorbeeldgedrag vertonen en hopen dat de medewerkers dit gedrag overnemen. De AP als CEO, zo simpel doet de AP dat.
Ik heb het jaarverslag AP 2022 (4) er toch maar even op nageslagen om het een en ander te checken en dan valt mij op dat het aantal meldingen van datalekken met vijftien procent is afgenomen, dat feit is wat mij betreft meer nieuws dan de datalekken bij de AP zelf. Opvallend is dat bij dit feit geen verklaring voor deze afname is gegeven. Hebben al die andere activiteiten die het AP uitvoert, anders dan de wettelijk taak, hun vruchten afgeworpen? Vreemd ook dat deze afname in datalekmeldingen dan weer niet in het nieuws, maar wel in deze achter het nieuws (AHN), komt!

Fook Hwa Tan - De Noodzaak van Maximale Transparantie bij Beveiligingsincidenten

In een tijd waarin cybercriminaliteit een constante dreiging vormt, is het begrijpelijk dat sommige organisaties terughoudend zijn om beveiligingsincidenten openbaar te maken. Het idee is dat het delen van dergelijke informatie aanvallers inzicht kan geven in zwakke plekken en hen kan aanmoedigen nieuwe methoden te ontwikkelen. Echter, deze opvatting is achterhaald. Aanvallers zijn al bekend met veel voorkomende kwetsbaarheden en maken gebruik van geavanceerde technieken om systemen binnen te dringen. Het verbergen van beveiligingsincidenten stopt hen niet, maar het houdt gebruikers wel in het ongewisse en voorkomt zo dat er passende maatregelen worden genomen.

Maximale transparantie is de sleutel tot een effectieve beveiligingsstrategie. Door beveiligingsincidenten openlijk te delen, kunnen organisaties van elkaars fouten leren en gezamenlijk werken aan verbeteringen. Dit bevordert een cultuur van verantwoording en continue verbetering op het gebied van gegevensbescherming. Bovendien stelt het gebruikers en klanten in staat om te begrijpen welke risico's ze lopen en stelt het hen in staat om passende maatregelen te nemen om zichzelf te beschermen.

Natuurlijk is er een balans nodig tussen transparantie en het voorkomen van verdere schade. Het is van cruciaal belang dat organisaties eerst de nodige stappen zetten om de oorzaak van het incident aan te pakken voordat ze dit openbaar maken. Bovendien moet gevoelige informatie, zoals persoonsgegevens, zorgvuldig worden behandeld en mag het delen van details geen onnodig risico vormen voor individuen of organisaties.

De beveiligingsincidenten bij de AP hadden wellicht eerder bekend moeten zijn, zodat passende maatregelen genomen konden worden. Door volledige openheid en transparantie na te streven, zetten we een belangrijke stap richting een veiligere digitale wereld. Het is hoog tijd dat alle organisaties, zowel publiek als privaat, deze benadering omarmen en samenwerken om onze systemen en gegevens beter te beschermen.

Lilian Knippenberg – Zo leidt transparantie daadwerkelijk tot betere veiligheid

Vroeger zeiden IT-ers nog tegen elkaar 'security by obscurity': houd zo veel mogelijk over je IT- infrastructuur geheim en je bent veilig. Gelukkig bewegen we nu als vakgebied naar 'security by design' en 'security by default': specifieke beveiligingsmaatregelen nemen en op die manier de veiligheid van je infrastructuur borgen. Ik hoop dat transparantie een onomstreden goed gaat worden, waarbij ook informatie over IOC 's '(indicators of compromise') door alle verdedigingsteams in de wereld wordt gedeeld. Dat zal nog wel even duren, want ook hier geldt het kat- en muisspel met criminelen. We willen de crimineel niet wijzer maken dan diegene al is. Natuurlijk geldt dat ook andersom: hoe weten wij wat de crimineel nog niet weet? Kunnen we dan niet beter alles delen wat we weten?

Ik vind het voorbeeld van de AP wat betreft het noemen van het aantal en de aard van de beveiligingsincidenten in het afgelopen jaar een goed voorbeeld. Maar let wel: in combinatie met andere tekenen van transparantie, zoals

het delen van technische informatie over kwetsbaarheden en IOC 's. Het landelijk dekkend stelsel van het NCSC speelt daarin wat mij betreft een cruciale rol. De sectorale insteek is logisch, maar ik zou ook graag zien dat verschillende sectoren van elkaar leren. Dan kunnen we als Nederland echt gezamenlijk optrekken en concurrentie op veiligheid achterwege laten. Gelukkig is daar nu al het Dutch Institute for Vulnerability Disclosure (DIVD). Vrijwilligers die Nederland een stukje veiliger maken door het opsporen van kwetsbaarheden en door de getroffen organisaties te informeren en te helpen. Zo kan transparantie zowel voorafgaand aan een incident (bij 'alleen' een kwetsbaarheid), als tijdens/achteraf (door het delen van IOC 's) en tot slot aan het eind van het jaar (bij het jaarverslag) leiden tot daadwerkelijk betere veiligheid.

Chris de Vries - Transparant zijn of niet?

We leven in een wereld waarin allerlei spelletjes worden gespeeld. Hoewel het verkleinwoord 'spelletjes' wordt gebruikt, is de inzet vaak enorm: zowel in financiële waarde als inzake imagoschade. Dus is het begrijpelijk dat geen enkele organisatie graag in de openbaarheid treedt wanneer het fout is gegaan en zeker niet wanneer de fout ook binnen de organisatie gezocht moet worden.

Binnen dat kader moet dan ook de discussie geplaatst worden over transparantie. De natuurlijke reactie is gesloten te blijven. Zo ook bijvoorbeeld in het bankwezen waarin het heel gebruikelijk was om negatief vermogen en negatieve jaarresultaten – met toestemming van de overheid – te camoufleren. Daartegenover staat het bedrijfsleven dat bij eenzelfde actie beticht zou zijn van bedrog, oplichting en fraude. Het argument om de wet verschillend uit te leggen voor in principe gelijke partijen: het publiek mocht het vertrouwen in het bankwezen niet verliezen.

En dus rijst de vraag hoe transparant is de AP in werkelijkheid. Wordt met het argument van (staats)veiligheid, vertrouwen behouden in en politieke voorbeeldfunctie wellicht het een en ander buiten de schijnwerpers gehouden? En zijn die argumenten valide? Wat verliezen wij aan vertrouwen als later alsnog de fouten boven tafel komen?

En over vertrouwen gesproken, het CBS publiceerde een vertrouwensoverzicht van Personen van 15 jaar of ouder (5) met als trieste instituties beneden de vijftig procent:

Instituten	Vertrouwen
Politici	23,8%
Kerken	29,6%
Tweede Kamer	30,4%
Grote Bedrijven	35,8%
Pers	39,8%
Ambtenaren	42,5%
Banken	48,5%
Europese Unie	48,7%

Vertrouwenstabel op basis van gegevens van het CBS.

Het hoogst scoorden (met scores boven de 75 procent): de gezondheidszorg (78,3%), de politie (77,0%) en rechters (76,6%). De vraag komt dus op of juist de formele staatsinstituties en het grote bedrijfsleven (inclusief banken) niet een veel verdergaande openheid moeten nastreven om het vertrouwen te herwinnen. Het vertrouwen kwam in de twintigste eeuw te voet en ging sinds circa 1987 te paard. Voor mij is het antwoord een volmondig 'ja'.

Referenties

(1) https://www.security.nl/posting/796706/Autoriteit+-Persoonsgegevens+vorig+jaar+slachtoffer+social+engineering-aanval
(2) https://www.security.nl/posting/795534/Cybercampagne+-Britse+overheid+leidt+naar+streaming-app+gebruikt+voor+piraterij
(3) https://nl.wikipedia.org/wiki/Autoriteit_Persoonsgegevens
(4) https://autoriteitpersoonsgegevens.nl/documenten/ap-jaarverslag-2022
(5) https://www.cbs.nl/nl-nl/nieuws/2023/19/minste-vertrouwen-in-tweede-kamer-in-10-jaar-tijd