Analyse Enquête
Bewustwording Cyberweerbaarheid

Inhoud

Bewustwording cyberweerbaarheid

IT beveiliging is een zeer actueel onderwerp met groeiende belangstelling, niet in de laatste plaats doordat geslaagde hacks op IT systemen bijna dagelijks in het nieuws zijn en ook de impact op de bedrijfsvoering laten zien. Om inzicht te krijgen in de noodzaak van het vergroten van de bewustwording van IT beveiliging in de regio Drechtsteden is door het samenwerkingsverband Cyber Netwerk Drechtsteden een enquête uitgezet met de volgende twee doelen:
1. Inventariseren in hoeverre er begrip is van de noodzaak/nut/belang van IT binnen de organisatie en de maatregelen die daarbij getroffen worden.
2. Vergroten bewustzijn inzake nut en/of noodzaak van de beveiliging van IT binnen de organisatie.

Van de 60 aangeschreven potentiele bedrijven hebben in totaal 38 respondenten de enquête ingevuld. Het betreft dus een kleine steekproef. Het is lastig speculeren of deze steekproef van 38 representatief genoemd mag worden voor de totale populatie. Zijn de respondenten positiever over de IT borging of zijn ze juist kritisch op hun eigen handelen en hebben ze daarom mee gedaan.

Deelnemers

Deze respondenten waren werkzaam bij bedrijven in de Drechtsteden (Alblasserdam (n=3), Dordrecht (n=5), Gorinchem (n=1), Hardinxveld-Giessendam (n=3), Hendrik-Ido-ambacht (n=4), Papendrecht (n=4), Sliedrecht (n=5), Zwijdrecht (n=3) en anders (n=10)). Het grootste gedeelte van de respondenten was directielid (n=18) of actief op de IT afdeling (n=13) van de bedrijven. De overige respondenten gaven aan werkzaam te zijn op de afdeling administratie (n=3), sales en marketing (n=1), productie (n=2) of overige.

De grootte van de bedrijven waar de respondenten werken varieerde sterk in het onderzoek. Zo waren er bedrijven met minder dan 5 medewerkers (n=3), tussen de 5-10 (n=2), 11-20 (n=6), tussen de 21-50 (n=9), 51-100 (n=3), 101-250 (n=8) en meer dan 251 (n=7).

Enquête

Alvorens uitspraken te kunnen doen over begrip van nut van IT en het vergroten van de bewustwording van de IT beveiliging is het van belang om inzicht te hebben in de betrouwbaarheid van de gebruikte vragenlijst, met andere woorden kan de vragenlijst een juiste uitspraak doen over de aspecten continuïteit en beveiliging van IT systemen. Een vragenlijst wordt als betrouwbaar gezien als de betrouwbaarheidsindex Cronbachs $\alpha > 0,7$ is. In dit geval is Cronbachs $\alpha = 0,826$ en kan gesteld worden dat de vragenlijst betrouwbaar is.

	If item dropped
	Cronbach's α
In welke mate ziet u IT als een kritische succesfactor voor uw bedrijf?	0.766
Staan beveiliging en continuÃ¯teit van IT op de agenda van de directie?	0.796
Is een inventarisatie van de belangrijkste systemen voor uw bedrijf uitgevoerd?	0.789
Is er een actueel overzicht van IT applicaties en systemen in uw organisatie aanwezig?	0.782
In welke mate zijn uw bedrijfsprocessen afhankelijk van IT?	0.771
Hoeveel schade loopt uw organisatie na 1 uur op als uw belangrijkste IT systemen uitvallen?	0.784
Hoeveel schade loopt uw organisatie na 1 dag op als uw belangrijkste IT systemen uitvallen?	0.771
Hoeveel schade loopt uw organisatie na 1 week op als uw belangrijkste IT systemen uitvallen?	0.781
In welke mate zijn uw bedrijfsgegevens vertrouwelijk en/of concurrentiegevoelig?	0.783
In welke mate werkt u met persoonsgegevens van zakelijke klanten of consumenten?	0.794
Hoeveel schade loopt uw organisatie op als bedrijfs- of klantgegevens op straat komen te liggen?	0.788
Is er een overzicht van de maatregelen om uw IT- en bedrijfsgegevens te beveiligen gedocumenteerd?	0.759
In welke mate is het beheer van IT uitbesteed?	0.826
Hoe 1 weet u dat de beveiliging van uw systemen op orde is?	0.798
Worden medewerkers getraind in de veilige omgang met IT en informatie?	0.776
Worden gebruikersaccounts met bijbehorende rechten tot systemen en applicaties periodiek beoordeeld?	0.796
Wordt de back-up procedure periodiek getest?	0.790
Is 2-factor authenticatie ingeregeld voor systemen en applicaties die van buitenaf benaderbaar zijn?	0.791
Worden beveiligingsupdates van systemen en applicaties uitgevoerd?	0.797
Zijn er maatregelen getroffen om in het geval van een IT-storing verder te kunnen werken en IT ook tijdig weer te herstellen?	0.788
Heeft u in het verleden te maken gehad met cybercrime?	0.808

RESULTATEN

De resultaten worden per onderwerp besproken. Er zijn vele analyses per vraag te maken op basis van de ingevulde antwoorden. Er is echter gekozen om de antwoorden te groeperen rondom de 2 hoofdonderwerpen van de enquête, te weten de status van IT in het bedrijf en een globale impact van cybercrime omdat de vragenlijst ook geënt was op het slechts inventariseren van de status van IT en kwetsbaarheid ervan in de Drechtsteden regio.

Actualiteit van IT in het bedrijf

Het gemiddelde antwoord op de vraag: ‘In welke mate zijn uw bedrijfsprocessen afhankelijk van IT?’ en ‘In welke mate ziet u IT als een kritische succesfactor voor uw bedrijf?’ ligt tussen de ‘hoog’ en ‘zeer hoog’. Dit antwoord wordt gedekt door een aantal andere gegevens uit de enquête. 97% van de bedrijven in de regio Drechtsteden heeft meer of minder recent een inventarisatie uitgevoerd van de belangrijkste systemen in het bedrijf. 89% van de bedrijven geeft aan een actueel overzicht te hebben van IT applicaties en systemen die in de bedrijven aanwezig is. Waar respondenten nog aangeven dat de hoeveelheid schade voor de organisatie, 1 uur na het uitvallen van de belangrijkste IT systemen nog ‘gemiddeld’ is dit na een dag al ‘hoog’ en na een week gaat het al richting ‘zeer hoog’. Het bewustzijn van de afhankelijkheid van IT wordt ook weerspiegeld doordat beveiliging van IT bij 92% van de directies van de bedrijven waar de respondenten werken op de agenda staat.

Men kent niet alleen de impact van de schade van IT systemen maar er worden ook diverse maatregelen getroffen om schade aan IT systemen te voorkomen.

- Bij alle respondenten (100%) worden er beveiligingsupdates van systemen en applicaties uitgevoerd.
- 92% van de respondenten geeft aan dat in hun bedrijf de gebruikersaccounts en de bijbehorende rechten tot systemen en applicaties periodiek worden beoordeeld.
- 88% geeft aan dat er maatregelen getroffen zijn om in het geval van een IT-storing verder te kunnen werken en IT ook tijdig weer te herstellen.

- 85% geeft aan dat de back-up procedure periodiek wordt getest.
- In 76% van de gevallen is er een 2-factor authenticatie ingeregeld voor systemen en applicaties die van buitenaf benaderbaar zijn.
- 63% van de respondenten geeft aan het personeel regelmatig te trainen in veilige omgang met IT en informatie.

Ondanks dit palet aan maatregelen die binnen de bedrijven gehanteerd wordt geeft 37% toch aan niet zeker te weten of de IT beveiliging op orde is in het bedrijf.

Bedrijfsgegevens kunnen vertrouwelijk of concurrentiegevoelig zijn. Van de geënquêteerden geeft slechts 1 van de respondenten aan dat zijn bedrijf geen vertrouwelijke of concurrentie gevoelige bedrijfsgegevens heeft, bij 20 respondenten zijn de bedrijfsgegevens deels vertrouwelijk en bij 17 respondenten volledig vertrouwelijk. Als we deze 2 laatste groepen naast elkaar zetten en kijken naar de actualiteit van IT dan geven de respondenten respectievelijk in 90% en in 94% van de gevallen aan beveiliging en continuïteit van IT op de agenda te hebben staan. Op basis van deze percentages kan niet gezegd worden dat de groep die meer gevoelige bedrijfsgegevens heeft IT continuïteit beveiliging vaker op de agenda heeft staan $t=0,35$ $(df=34)$, $p > 0,05$.

Vier respondenten geven aan dat hun bedrijf geen gevoelige informatie van klanten behandelt, 20 respondenten geven aan regelmatig gevoelige klanteninformatie te hebben en 14 respondenten geven aan altijd gevoelige klantinformatie te gebruiken. Vreemd genoeg geeft maar 85% van de laatste groep aan, continuïteit van IT en IT beveiliging en op de agenda te hebben staan, terwijl bij de groep die slechts regelmatig klantgegevens op de systemen heeft, dit 95% is. Dit verschil is echter niet significant($t=0,85$ $(df=20)$, $p > 0,05$).

Cybercrime

44% van de respondenten heeft in het verleden te maken gehad met cybercrime. De geregeld genoemde vormen van cybercrime zijn virussen, ransomware, phising, spookfacturen.

Van de groep die in het verleden met cybercrime te maken heeft gehad staat IT en beveiliging in 88% van de gevallen structureel op de agenda staan en van de groep die geen ervaring met cybercrime heeft gehad is dit weliswaar op basis van de steekproef iets hoger, nl 95% maar dit verschil is echter niet significant $t=0,75$ $(df=27)$, $p > 0,05$

Gegevens tonen aan dat het percentage van de groep die volledige vertrouwelijk informatie heeft dat weleens te maken heeft gehad met cybercriminaliteit (47%) groter is dan dit percentage in de groep bedrijven waar slechts gedeeltelijk vertrouwelijke informatie is (40%). Echter dit verschil is niet significant ($t=-0,42$ $(df=34)$, $p > 0,05$).

Als het gaat om preventie van cybercrime door te investeren in de beveiliging van IT systemen zien we dat 37% van de respondenten, op vraag ‘hoeveel % van uw IT kosten wordt besteed aan beveiliging’ aangeeft dit niet te weten. Dit wil natuurlijk niet zeggen dat er geen uitgave gemaakt worden voor de beveiliging. 1/3 van de respondenten zegt tussen 0 en 10% van de IT kosten te besteden aan beveiliging en 1/3 tussen de 10 en 20%. Uit de data kan niet geconcludeerd worden dat de uitgave voor IT beveiliging hoger is bij bedrijven die zeer vertrouwelijk bedrijfsgegevens hebben of die in het verleden te maken hebben gehad met cybercrime. Ook bij deze groep bedrijven zijn 4 respondenten niet op de hoogte van deze uitgaven.

CONCLUSIE

Het eerste doel van dit onderzoek was het inventariseren van het nut/noodzaak/belang van IT binnen de organisatie en de maatregelen die daarbij getroffen worden. Aan de hand van de gegeven antwoorden van de respondenten kan geconcludeerd worden dat, gezien men in hoge tot zeer hoge mate afhankelijk is van IT, de beveiliging van IT systemen bijna bij alle respondenten op de agenda staat maar ook dat bij bijna alle respondenten een actueel overzicht aanwezig heeft van IT applicaties en systemen. Daarnaast neemt het overgrote deel adequate maatregelen om de beveiliging op orde te houden. De aanwezigheid van gevoelige bedrijfsinformatie of klanteninformatie leidt niet tot een prominentere plaats van IT-beveiliging op de agenda in vergelijking met bedrijven met minder gevoelige gegevens.

Ondanks dat een behoorlijk deel van de bedrijven te maken heeft gehad met cybercrime is het niet zo dat IT-beveiliging bij deze bedrijven vaker op de agenda staat. Dit is naar zeggen bij bijna alle bedrijven een agendapunt. Hoe deze agenda-aanwezigheid zich vertaalt in acties is niet uit de enquête af te leiden. Dat deze aanwezigheid op de agenda nog geen garantie biedt blijkt uit het feit meer dan een derde van de respondenten niet zeker te weten of de IT beveiliging op orde is. De reservering voor IT-beveiliging zijn niet anders voor bedrijven met gevoelige bedrijf- of klantennformatie.

Het tweede doel, het vergroten van het bewustzijn inzake nut en/of noodzaak van de beveiliging van IT binnen het bedrijf wordt behaald door het lezen en beantwoorden van de enquête. Echter, dit gebeurt louter door de respondent. Het succes van cybersecurity of cyber weerbaarheid ligt niet in de handen van één persoon van het bedrijf die bepalend of verantwoordelijk is voor de IT, laat staan bij aanwezigheid van IT op de directie-agenda, maar is de resultante van de dagelijkse gedragingen van alle werknemers van het bedrijf. Over de cyber weerbaarheid van de werknemers kan deze enquête helaas geen uitspraak doen.

ADVIES VOOR VERVOLGONDERZOEK

Deze enquête is een eerste aanzet om te komen tot een veiliger bedrijfsklimaat op IT gebied in de Drechtstedenregio. Om meer inzicht te krijgen in het online veiligheidsgedrag van werknemers is er een gevalideerd meetinstrument, de online security behaviors (SeBis). Dit instrument kan worden gebruikt om een uitspraak te doen over de actuele gedragsintenties ten aanzien van veiligheid. Als deze door een substantieel deel van de werknemers, die betrokken zijn bij IT handelingen, wordt ingevuld kan een gerichtere uitspraak gedaan worden over de cyber weerbaarheid van het bedrijf of de Drechtstedenregio bedrijven in zijn algemeenheid.

Online security behaviors (SeBIS)

Geef jouw reactie op de volgende stellingen met het antwoord dat het meest van toepassing is:

(1) Nooit, (2) Zelden, (3) Soms, (4) Vaak, (5) Altijd.

1. Wanneer ik er op word gewezen om een software update te installeren dan doe ik dat meteen (Updating)
2. Ik probeer er voor te zorgen dat de programma's die ik gebruik up-to-date zijn. (Updating)
3. Ik sluit mijn computerscherm altijd handmatig af, wanneer ik er van wegloop. (Device Securement)
4. Als ik voor een iets langere periode geen gebruik maak van mijn computerscherm dan is mijn scherm automatisch 'gelocked'. (Device Securement)
5. Ik gebruik een PIN of een passcode om mijn telefoon te beveiligen. (Device Securement)
6. Ik gebruik een PIN of een passcode om mijn tablet of laptop te beveiligen.
7. Als ik een security probleem ontdek, ga ik verder met waar ik mee bezig was. Met de gedachte: iemand anders pakt dat probleem wel op. (Proactive Awareness)
8. Als iemand me een link stuurt open ik die zonder eerst te verifiëren waar de link naartoe leidt. (Proactive Awareness)
9. Ik ga na of mijn anti-virus software zichzelf regelmatig update. (Updating)
10. Als ik door websites browse, dan ga ik eerst met mijn muis over de links om te zien waartoe ze leiden, alvorens ik er op klik. (Proactive Awareness)
11. Ik baseer de veiligheid van een website op de uitstraling van de website en het gevoel dat ik er bij heb in plaats van dat ik let op de URL bar. (Proactive Awareness)
12. Ik verander pas mijn wachtwoorden als het moet. (Password Generation)
13. Ik gebruik verschillende wachtwoorden voor de verschillende sites en accounts die ik gebruik. (Password Generation)
14. Ik gebruik geen speciale karakters in mijn wachtwoord als er niet om wordt gevraagd. (Password Generation)
15. Als ik een nieuwe online account aanmaak dan probeer ik het wachtwoord complexer op te stellen dan dat de website waar het wachtwoord voor is vraagt. (Password Generation)
16. Ik voed websites met informatie zonder dat ik er op let of die informatie veilig gebruikt gaat worden. (Proactive Awareness)

Werkgever

17. Mijn werkgever geeft mij de handvatten om cyber secure te werken
18. Er worden trainingen of workshops georganiseerd zodat cyber secure werken wordt aangemoedigd
19. Mijn werkgever heeft maatregelen getroffen om IT en bedrijfsgegevens te beveiligen
20. Deze maatregelen zijn inzichtelijk voor het personeel
21. Het zit in de bedrijfscultuur om cyber secure te werken
22. Als ik cybercrime vermoed weet ik waar ik moet aankloppen
23. Als ik cybercrime vermoed weet ik wat ik moet doen