Overzicht resultaten onderzoeksronde 1 Cybersecurity

12.05.18

Inleiding

In Nederland en in Limburg wordt sinds kort tijd veel aandacht besteed aan cybercrime. Het Platform Veilig Ondernemen Limburg laat een onderzoek uitvoeren naar de manier waarop Limburgse ondernemers met cybercriminaliteit omgaan. Dit onderzoek omvat twee rondes. De gedachte is om te kijken of er gedurende het jaar, met name door de publiciteit rondom de AVG, iets veranderd in de mate waarin ondernemers actief bezig zijn met de risico's van cybercrime. De eerste ronde is in maart uitgevoerd, de tweede ronde zal na de zomer plaatsvinden. In het onderstaande een samenvatting van de resultaten van de eerste ronde.

Bevindingen

De verdeling van de respondenten (max. 409) m.b.t de bedrijfsomvang is niet helemaal conform de werkelijke Limburgse verdeling. 46% van de respondenten geeft aan zzp-er te zijn, dat ligt in werkelijkheid iets hoger (volgens TO) en het aandeel grotere bedrijven bij de respondenten is groter dan in werkelijkheid.

In het onderzoek is gekeken naar verschillende thema's:

1. Inschatting van het risico voor de eigen onderneming en de verwachte (of ervaren) schade door cybercriminaliteit.
    a. 39% acht het onwaarschijnlijk dat ze slachtoffer worden van cybercriminaliteit en 25% scoort neutraal.
    b. 32% heeft geen drijfveer om zich met cybercriminaliteit bezig te houden. Van de ondernemers die dat wel doen zijn de nieuwe privacywet, reputatieschade en interne datalekken ongeveer even grote drijfveren.
    c. De grootste risico's zien ondernemers bij hun eigen administratieve systeem (60%) en bij hun administratieve verwerking van klantgegevens (54%) productiefaciliteiten scoren laag (15%) en kassasystemen, webshops e.d. net iets meer (22%)
    d. De meeste schade zien ondernemers op het vlak van reputatie (45%) en direct en indirect productieverlies (resp. 37% en 25%).
    e. Dat de meeste ondernemers vooral op hun eigen onderneming gefocust zijn blijkt uit het feit dat 60% aangeeft geen idee te hebben hoe hun leveranciers omgaan met hun gegevens. Bij kleinere ondernemingen speelt dat het meest.

2. Mate waarin ondernemers slachtoffer zijn geweest van cybercriminaliteit.
    a. Slechts 17% van de ondernemers zegt slachtoffer geweest te zijn van cybercriminaliteit, 22% van pogingen tot (phishing e.d.), de rest niet. Dat ligt wel in lijn met het landelijke cijfers.
    b. Als het gaat om het soort criminaliteit bij de slachtoffers scoort phishing het hoogst (46%) daarna ransomware (35%) oplichting (17%) en het uit de lucht halen van de website (14%).

3. Genomen maatregelen
    a. De maatregelen die men neemt liggen vooral op het technische vlak (84%), organisatorische maatregelen (wachtwoorden verplicht veranderen e.d.) scoort 31%. Educatie van medewerkers ligt bij 16%, juridische maatregelen (m.n. AVG) zit op 12%.
    b. Naarmate de bedrijven groter zijn worden er meer maatregelen genomen en is er meer aandacht voor beveiliging.
    c. Op het gebied van privacy is slechts 19% bewust actief met o.a. de AVG. Daarbij geldt hoe groter, hoe actiever.

4. Eigen informatievoorziening en behoefte aan ondersteuning
    a. De informatievoorziening loopt vooral via vakliteratuur en een meerderheid (55%) geeft aan geen behoefte te hebben aan extra ondersteuning.

b. Als er informatie komt zou dat via de branche moeten lopen en herkenbaarheid van betrouwbare tools (software) wordt aangegeven als item daarbij.
c. De kleinste groep nee-zeggers zit bij de bedrijven met tussen de 5-20 mensen personeel.

Conclusies
Uit de cijfers kun je afleiden dat het bewustzijn rondom cybercrime wel een extra zetje kan hebben. De ondernemers die zeggen dat het onwaarschijnlijk is dat ze slachtoffer worden of neutraal scoren vormen samen een groep van meer dan 60%, 1/3^{e} ziet ook geen noodzaak om er wat aan te doen. En dat terwijl ook in Limburg (net als landelijk) 1 op de 5 bedrijven slachtoffer wordt van cybercrime. Dat geven de ondernemers in dit onderzoek zelf aan.

Meer dan de helft zegt ook geen behoefte te hebben aan ondersteuning. Dan hebben we het in Limburg over meer dan 40.000 bedrijven. De groep bedrijven met tussen de 2 en 20 mensen laat een iets ander beeld zien, minder 'nee'. Vraag is nog of dit voortkomt uit een lage risicoperceptie. Hoe groter de bedrijven hoe actiever. Bij de bedrijven met meer dan 20 medewerkers heeft meer dan 90% de beveiliging van data formeel geregeld.

Wat opvalt is dat de overgrote meerderheid (84%) met name technische maatregelen noemt. Organisatorisch is al een stuk minder (31%) en educatieve maatregelen nog minder. Terwijl de ervaring leert dat 80% van de problemen ontstaan door menselijke fouten. De vraag is of hier een latente behoefte ligt in de vorm van training en instructie voor medewerkers. Het kan een strategie zijn om de kans op fouten kleiner te maken door technische oplossingen.

Verder zien we dat een meerderheid geen zicht heeft op manier waarop leveranciers met hun gegevens omgaan. Het is interessant om te zien of dat in het najaar minder is geworden als het stof rondom de handhaving van de AVG is neergedaald.

Bij bedrijven met meer personeel zie je ook –niet onverwacht- meer bewustzijn. Ze geven vaker aan maatregelen te nemen en verantwoordelijkheden rondom bijv. De privacywetgeving ook belegd te hebben bij personen.

Bijlage

Antwoorden samengevat

A. Kans op…
    a. 39% niet waarschijnlijk, 25% neutraal, 33% waarschijnlijk
    b. 32% geen drijfveer
B. Risico
    a. 60% eigen administratief systeem
    b. 54% verwerking van klantgegevens, 15% produktie, 22% anders zoals kassa, webshop
    c. zonder ICT kan 28% langer dan een dag, 22% 104u, 21% < 1u
C. Schade
    a. Reputatie 45%, productieverlies 37%, 25%, indirect prod verlies 28% anders
D. Databeveiliging leveranciers
    a. 60% niet
        i. kruis: b-to-b bewuster mee bezig m verschil is klein
        ii. kruis: meer personeel, meer zicht op leveranciers
E. slachtoffer
    a. 17%, 22% mislukt (phishing vooral), 55% nee
    b. grotere bedrijven meer pogingen, slachtoffers 20-30%, weinig verschil in grootte bedrijf
F. soort
    a. phishing: 46%, ransomware 35%,17% oplichting, 14% website
G. maatregelen
    a. 84% technisch, 31% organisatorisch, 16% educatie, 12% juridisch
        i. b-t-b scoren hoogst op maatregelen
        ii. meer personeel, meer maatregelen
H. info via
    a. vakliteratuur 37%, IT leverancier 28% + 20% gesp. Leveranciers
I. privacy
    a. 19% echt mee bezig
    b. meer personeel, bewuster mee bezig, boven 100, 90% actief
J. hulp
    a. 59% nee, 13% ja, via branche, 11% goede herkenbaarheid v tools
    b. vraag zit vooral bij bedrijven 2-20 personeel