INFORMATIEBEVEILIGING, CYBERSECURITY & AVG

WAAROM INFORMATIE-BEVEILIGING ONDERDEEL MOET ZIJN VAN DE BEDRIJFSCULTUUR

Informatiebeveiliging, cybersecurity en AVG zijn voor veel accountants abstracte en ongrijpbare onderwerpen. Ze hebben het imago geen directe bijdrage te leveren aan de kwaliteit van de dienstverlening van het kantoor. In de praktijk worden ze daardoor vaak beschouwd als bijzaak, een hinderlijke drempel of een separaat traject wat wordt overgelaten aan de (externe) IT-manager. Het ontbreken van een helder beleid en aandacht voor informatiebeveiliging leidt ertoe dat gebruikers zich onvoldoende bewust zijn van de risico's en zich daardoor (onbewust) niet veilig gedragen.

Informatiebeveiliging, met specifieke aandacht voor cybersecurity en AVG, gaat niet alleen over ICT-systemen. Het gaat over de beschikbaarheid, integriteit en vertrouwelijkheid van informatie en infor-matiesystemen waarop de dienstverlening van het kantoor is gebaseerd. Dit gaat verder dan alleen het beheer van de software en netwerk van het kantoor.
Het omvat ook het uitwisselen van informatie via e-mail en diensten zoals Skype, Teams en Whatsapp, het gebruik van websites en zoekmachines, het gebruik van social media zoals Facebook, Instagram, LinkedIn en Twitter en de kaders waarbinnen dit alles wordt gedaan.

Risico's veranderen continu doordat doelstellingen, interne en externe dreigingen, de omgeving en wet- en regelgeving (o.a. AVG) veranderen. Als onvoldoende rekening wordt gehouden met de veranderende risico's, zijn maatregelen op termijn niet meer passend. Informatiebeveiliging vergt daarom een cyclisch, iteratief en terugkerend proces met als doel risico's te mitigeren.

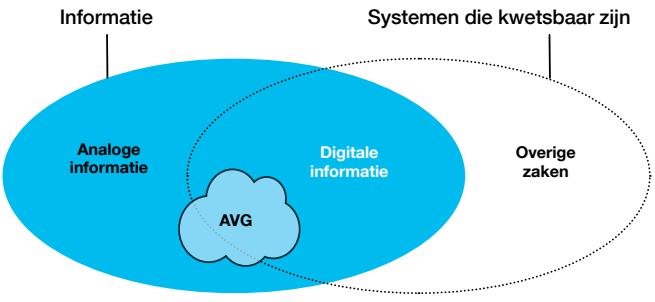
DIGITALE WEERBAARHEID VAN KANTOREN

De digitale weerbaarheid van accountantskantoren staat onder druk door een toenemende complexiteit en connectiviteit in het IT-landschap, nieuwe ontwikkelingen en door te weinig aandacht voor digitale veiligheid bij nieuwe, innovatieve projecten.

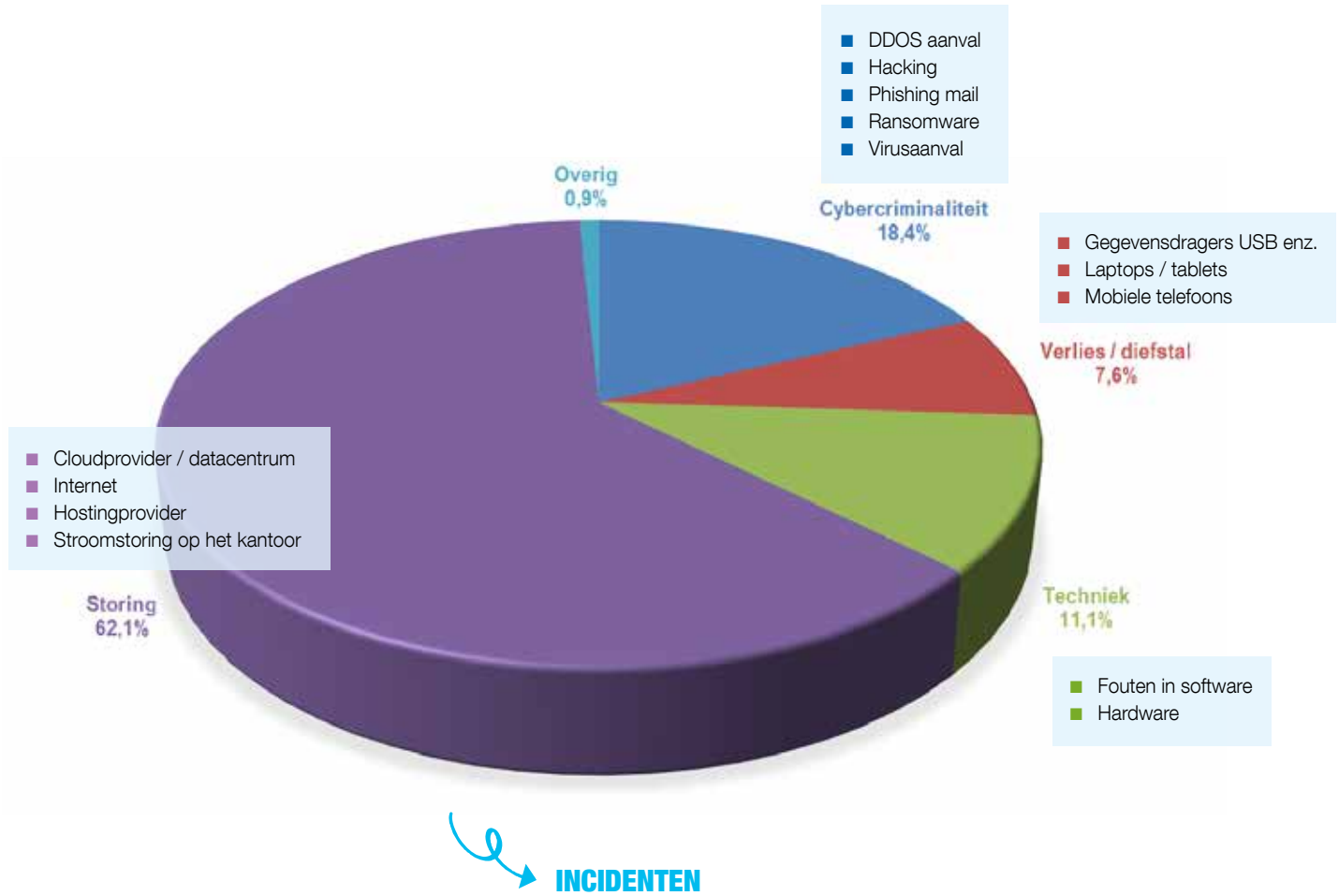
Onvoldoende aandacht voor deze ontwikkelingen en gebrek aan inzicht in de risico's maakt accountantskantoren kwetsbaar voor cybersecurity- en privacy-incidenten: incidenten waarvan de gevolgen groot kunnen zijn voor de kwaliteit van de dienstverlening, het vertrouwen door de klant in het kantoor en de continuiteit van de organisatie. Crisissituaties zoals het coronavirus maken dit extra duidelijk waarbij ineens de werksituatie van kantoor verandert naar thuiswerken.

HET BELANG VAN CULTUUR

In de waan van dag zien we dat de aandacht voor informatiebeveiliging zich vaak beperkt tot de aanschaf van een of meer technische tools. De belangrijkste factoren voor het slagen van informatiebeveiliging zijn de kennis en het bewustzijn van medewerkers, hoe zij omgaan met risico's, hoe zij de processen en procedures inrichten en de wijze waarop de techniek dit ondersteunt. Om dit te kunnen realiseren, moet informatiebeveiliging een onderdeel worden van de cultuur van het kantoor. Zonder deze cultuur is het niet goed mogelijk risico's identificeren en te mitigeren. Het creëren van een cultuur van informatieveiligheid begint bij het ontwikkelen van een helder beleidskader dat wordt gedragen door het management.



INFORMATIEBEVEILIGING



INCIDENTEN

Uit onderzoek onder SRA-kantoren, het SRA-IT-Benchmark 2019, blijkt dat 18,4% van alle problemen met de IT-systemen in de laatste twaalf maanden waarmee het kantoor te kampen heeft gehad, is gerelateerd aan cybercriminaliteit.

VIJF STAPPEN OM SECURITY AWARENESS TE VERGROTEN

1. **Bepaal het gewenste niveau van bewustzijn**
   Voer een risico-inventarisatie uit en stel vast welke maatregelen zijn getroffen. Houd daarbij ook rekening met het risicobewustzijn. Het realiseren van een cultuurverandering waarbij informatieveiligheid een tweede natuur wordt, vergt niet alleen doelstellingen, maar ook continue betrokkenheid en draagvlak van het management.
2. **Inventariseer hoe ver u van het doel bent verwijderd**
   Als de doelstelling is bepaald, bepaal dan waar u staat. Kijk hiervoor bijvoorbeeld naar de huidige incidenten en het aantal datalekken. Neem eventueel de proef op de som. Hoe lang duurt het voordat een gevonden USB-stick wordt gerapporteerd of wat is de clickratio in een phishingtest?
3. **Bepaal hoe u de 'awareness gap' gaat overbruggen**
   Verschillende type medewerkers vergen een verschillende aanpak. Zorg voor het juiste moment om informatiebeveiliging onder de aandacht te brengen. Bijvoorbeeld na een incident of voor een drukke periode. Leg niet zo maar regels op, leg ze niet alleen uit maar ook hoe tot dit besluit is gekomen.
4. **Maak een plan van aanpak**
   Communiceer duidelijk over de plannen en de doelstellingen en zorg dat iedereen wordt betrokken. Denk hierbij aan verschillende werkvormen voor verschillende doelgroepen.
5. **De kracht van herhaling**
   Herhaal het awarenessprogramma regelmatig. Evalueer de resultaten en stel waar nodig bij.

MEER WETEN EN HOE NU VERDER?

Ga naar de AVG-dossierpagina op www.sra.nl/avg voor alle vragen en antwoorden en beschikbare documenten
of neem contact op met Tony van Oorschot,
automatisering@sra.nl.

10 AVG-RISICO'S

Risico's waar we vaak niet aan denken:

1. Bestanden belanden in de prullenbak
2. Gebruik van privé-USB-sticks, externe harde schijven en cd-rom's
3. Gebruik van bedrijfsapparaten voor privédoeleinden
4. Gebruik van persoonlijke e-mailaccounts voor het werk
5. Een eenvoudig centraal wachtwoord voor iedereen voor alles
6. Gastvrijheid op het kantoor 'Kom binnen!'
7. Te veel informatie verstrekken via de telefoon
8. Chaos op de (thuis)werkplek
9. De overvolle mailbox
10. Datalekken verzwijgen