In een serie van drie blogs voor de SRA-website (www.sra.nl/blog) hebben we in de afgelopen maanden informatiebeveiliging belicht vanuit drie verschillende perspectieven. In het eerste blog hebben we aandacht besteed aan social engineering, het belang van security awareness en de factor 'mens'. In het tweede blog hebben we het gehad over technische maatregelen om klantenportalen te beschermen. In het derde blog zijn we vervolgens ingegaan op de manier waarop organisaties omgaan met beveiligingsbeleid. Dit artikel brengt deze drie perspectieven samen.

Informatiebeveiliging:
Een goede balans tussen mens, techniek en organisatie

Op het gebied van informatiebeveiliging is techniek (IT) een belangrijk gereedschap waarmee toegang tot informatie kan worden verschaft. Daarnaast geeft techniek ons de middelen in handen om de vertrouwelijkheid, betrouwbaarheid en integriteit van deze informatie goed te regelen. Tot voor kort werd er door organisaties, daar waar het gaat over beveiliging, buitenproportioneel veel geïnvesteerd in techniek. Ook bij accountantskantoren was dat het geval en is dat wellicht nog steeds wel zo.

Meer dan alleen techniek (IT)

De buitenwereld vraagt steeds meer 'openheid' en toegang van buitenaf via internet. Dit vraagt om aanpassing van beveiligingsmaatregelen. Ook interne veranderingen binnen het kantoor kunnen vragen om dergelijke aanpassingen. Deze beveiligingsmaatregelen hebben vervolgens, omdat IT tegenwoordig in nagenoeg alle lagen van het kantoor is doorgedrongen, weerslag op alles en iedereen binnen het kantoor. Hierbij worden de nodige technische (IT-)maatregelen genomen om de boel te beveiligen. Maar zoals de beroemde hacker Kevin Mitnick ooit stelde: "Hoe goed beveiligd een fort ook is, als iemand de deur voor je openhoudt staan alle technische maatregelen buiten spel". Bij informatiebeveiliging draait alles om de zwakste schakel en die zit vaak niet (alleen) in de techniek.

Het gedrag van mensen wordt vaak als de zwakste schakel in de beveiligingsketen gezien, omdat dit gedrag in vergelijking met de techniek onvoorspelbaar is en mensen bovendien fouten kunnen maken. Hoe kwetsbaar ook, mensen en hun gedrag zijn een onlosmakelijk onderdeel van de beveiligingsketen. Veel informatiediefstal is gericht op het 'exploiteren' van de menselijke schakel. De meeste organisaties gebruiken processen en procedures om mens en techniek op een gecontroleerde manier te verbinden. Maar alleen

met processen en procedures ben je er nog niet: voldoende niveau van beveiligingsbewustzijn bij medewerkers is enorm belangrijk.

Meer dan alleen losse schakels

Onze stelling is dat informatiebeveiliging vraagt om een drieledige aanpak waarbij voldoende aandacht is voor het samenspel van mens, techniek en organisatie. Juist een effectief samenspel tussen deze drie schakels maakt het kantoor weerbaarder voor zaken die fout (kunnen) gaan. Om hierop te kunnen sturen is het verstandig een op maat gemaakt beveiligingsraamwerk op te stellen waarin de kwetsbaarheden van het kantoor concreet worden gemaakt. Deze kwetsbaarheden worden gerelateerd aan zowel de technische aspecten als de inrichting van processen en de naleving van processen. De kern van deze aanpak is het borgen van de menselijke interactie met techniek door middel van een passend geheel van afspraken. In tegenstelling tot een aanpak met een focus op technische maatregelen ontstaat hierdoor een kantoorbreed model voor informatiebeveiliging waarin de factoren mens, techniek en organisatie in samenhang worden beschouwd.

Meer dan alleen invoeren

Informatiebeveiliging is een onderwerp dat aan belang toeneemt en waarover de inzichten in hoog tempo veranderen. Zoals hierboven beschreven is de factor mens erg veranderlijk. Ook de stand van de techniek evolueert voortdurend. Wat gister niet kon is vandaag mogelijk. Daardoor veranderen dus ook de mogelijkheden en onmogelijkheden voor accountantskantoren. Het krijgen en houden van grip op informatiebeveiliging is een continu proces. De zogenaamde 'Plan-Do-Check-Act'-cyclus, die je ook op het onderwerp informatiebeveiliging kunt loslaten, beschrijft in dit kader een cyclus van voortdurende herijking van beveiligingsmaatregelen. Hierdoor ontwikkelen de beveiligingsmaatregelen zich verder en houdt een kantoor het onderwerp informatiebeveiliging levend en up-to-date. Het cruciale element van de 'Plan-Do-Check-Act'-cyclus is de 'Check': een fase die ons als accountants moet aanspreken. Met 'Check'-fase wordt het continu monitoren en evalueren van de ingestelde beveiligingsmaatregelen bedoeld. Dit kan worden geoperationaliseerd door bijvoorbeeld met enige regelmaat een (onafhankelijke) beveiligingsscan uit te voeren.

Bij het alleen laten uitvoeren van dergelijke scans is de kans aanwezig dat het samenspel tussen mens, techniek en organisatie op de achtergrond raakt. Dat moet niet en er is dan ook een ontwikkeling in de markt gaande dat softwareoplossingen beschikbaar komen die de drie factoren mens, techniek en organisatie overzichtelijk in een dashboard weergeven: een zogenaamd Security Operations Control Center of SOC.

Gedrag van mensen zwakste schakel

In het verleden waren SOC-oplossingen erg bewerkelijk, kostbaar en alleen van meerwaarde voor hele grote organisaties, de multinationals onder ons. Inmiddels zijn er oplossingen beschikbaar die zich meer en meer richten op het (grotere) mkb en daarmee dus zeker ook op accountantskantoren. Het dashboard levert een doorlopend inzicht in de stand van beveiligingszaken en maakt het daarmee mogelijk om sneller bij te sturen indien nodig. Iets wat met de steeds sneller veranderende (beveiligings)wereld meer dan welkom is!

Meer dan alleen de som der delen

Informatiebeveiliging is een kwestie van mens, techniek en organisatie, we kunnen het niet vaak genoeg herhalen. Het omvat het hele kantoor en is niet beperkt tot een losstaand project of product. Om uw klanten op een betrouwbare wijze te kunnen blijven bedienen, is het een onderwerp dat aandacht verdient. In die zin verrichten wij in dit artikel wat missiewerk voor het onderwerp. Door te zoeken naar een gebalanceerde mix van beveiligingsmaatregelen en deze balans continu te monitoren kan de kwaliteit van de informatiebeveiliging duurzaam worden verbeterd. Gebruik van een SOC-pakket kan uitkomst bieden door duidelijk zicht te geven in de factoren mens, techniek en organisatie, zodat zij in samenspel meer kunnen zijn dan de som der delen! ■

Dit artikel is geschreven door Age-Jan van der Meer, partner van KoutersVanderMeer, en Richard de Goede, adviseur bij Insite Security.

Meer informatie

Heeft u vragen of wilt u meer informatie over informatie-beveiliging neem dan contact op met SRA, Tony van Oorschot: tvanoorschot@sra.nl, of 030 656 60 60.