Ties Voskamp en Jeroen Kuper
Informatiebeveiliging is een hot topic, helemaal sinds de komst van de Wet meldplicht data-lekken begin dit jaar

Veranker informatie-beveiliging in je organisatie

Digitalisering zorgt niet alleen voor meer data, maar ook voor nieuwe manieren om al deze data te gebruiken en te delen. Informatiebeveiliging is dan ook een hot topic, helemaal sinds de komst van de Wet meldplicht datalekken begin dit jaar. Onafhankelijk IT & Security Consultant Ties Voskamp en Jeroen Kuper, Prestatieverbeteraar voor KoutersVanderMeer, zien dit voor accountants-kantoren vooral als een kans om zich te onderscheiden.

Hackers en cybercriminelen zijn bijzonder vindingrijk. Heb je net een effectieve beschermende muur rond je organisatie opgetrokken, komen ze weer met andersoortige aanvallen. De hype van het moment is ransomware, een chantagemethode op basis van besmette bestanden. “Deze vorm van besmetting kan op uiteenlopende manieren een organisatie binnenkomen en gijzelt bestanden op de computer van de ontvanger of een heel netwerk”, legt Jeroen Kuper uit. “Je ontvangt bijvoorbeeld via e-mail een betalingsherinnering, voor de meeste mensen een prikkel om direct te reageren. Zodra je het bestand opent, wordt er een virus geïnstalleerd dat je bestanden blokkeert en pas weer vrijgeeft na betaling van ‘losgeld’, meestal in de vorm van bitcoins.” Tenminste, in het gunstigste geval. Kuper wil maar zeggen: zo eenvoudig kan het gaan.

Van binnen naar buiten

Na besmetting via ransomware is het enige alternatief voor betalen het terugzetten van de back-up, maar daarmee verlies je hoe dan ook een paar dagen werk. Als je tenminste regelmatig een back-up

draait, anders kan de schade nog veel groter zijn. Bovendien is het kwaad al geschied. Doen we met zijn allen wel voldoende om bedreigingen als deze te voorkomen? “De meeste organisaties beveiligen van buiten naar binnen en zijn daardoor redelijk goed beschermd tegen gevaren vanaf het internet”, stelt Ties Voskamp. Natuurlijk loopt hij nog regelmatig tegen schoonheidsfoutjes aan, maar schokkende hiaten in de harde schil komt hij nauwelijks meer tegen. “Maar daarmee ben je er niet”, waarschuwt Voskamp. De beveiliging van de informatie die op andere manieren binnenkomt, intern wordt verspreid of van binnen naar buiten gaat, vindt hij minstens zo belangrijk. En juist daar gaat het nogal eens mis. Dat blijkt wel uit het ‘succes’ van ransomware.

M&M’s

De netwerken van organisaties doen volgens Voskamp vaak denken aan M&M’s: hard van buiten en zacht van binnen. Goed beschermd tegen online gevaar, maar als een bedreiging eenmaal binnen is – en dat kan dus al via een simpele e-mail – blijkt de beveiliging helemaal niet zo sterk. Ransomware krijgt de kans om bestanden te versleutelen, of denk aan kwaadaardige software die heimelijk data verzamelt. Mensen zijn in dit opzicht vaak de zwakke schakel. Medewerkers die informatie delen of een bestandje in de mail openen, zonder stil te staan bij de gevolgen. “Menselijke kwetsbaarheden zijn niet allemaal met technische middelen te ondervangen”, aldus Kuper. “Dit komt deels door het spanningsveld tussen beheersing en gebruiksgemak.” Een goed voorbeeld zijn macro’s die bepaalde handelingen automatisch uitvoeren. Handig, maar hierdoor hoeven hackers ook slechts één stap te zetten: een bestandje sturen en de rest gaat vanzelf.

Kwetsbaarheid

Hoe kun je je als organisatie dan nog meer tegen kwetsbaarheden van mensen wapenen? “Op de eerste plaats met trainingen en het creëren van bewustwording”, aldus Voskamp. “Pak dit vooral praktisch aan: laat medewerkers ervaren wat de consequenties van hun handelen zijn. Stoppen ze een onbekende usb-stick in hun computer? Confronteer ze dan met de mogelijke gevolgen. Zorg verder voor een open cultuur waarin medewerkers fouten mogen maken en problemen durven aankaarten. Alleen dan kun je als bedrijf adequaat reageren. Kortom, investeer in je ‘human firewall’.”

Daarnaast kan het fragmenteren of segmenteren van rechten heel effectief zijn, vult Kuper aan. “Hoe meer gebruiksrechten een medewerker heeft, hoe meer schade hij of zij kan veroorzaken, ook al is het niet kwaadwillend. Medewerkers willen over het algemeen overal bij kunnen, maar dat is een risico. Door barrières aan te brengen, meer gelaagdheid te creëren en scherper toezicht te houden op het uitgaande verkeer, kun je besmetting en/of de impact daarvan op het netwerk doorgaans voorkomen. Dit is geen eenmalige actie, maar net als de beveiliging met technische middelen een continu proces. Anders gezegd: zorg ervoor dat je informatiebeveiliging op alle manieren in je organisatie verankert.”

Zelf doen versus uitbesteden

De keuze daarbij is: zelf doen of uitbesteden. In het licht van de nieuwe wetgeving en technologie is het bijna onmogelijk om alles zelf te doen. Daarbij is uitbesteden dankzij schaalbaarheid ook voor het midden- en kleinbedrijf tegen behapbare kosten mogelijk. Kuper: “Denk wel heel goed na over wat je niet meer zelf wilt doen. Het vertrekpunt is dat je je verantwoordelijkheid niet kunt uitbesteden. Zorg er dus voor dat je altijd de regie houdt over wat je buiten de deur regelt. Weet waar je data zich bevindt en maak afspraken over wat anderen met jouw data mogen doen. Sta je bijvoorbeeld bewerkingen toe, of het gebruik van onderaannemers? Dat zijn belangrijke afwegingen.”

Volgens Kuper gaat het vaak fout op de koppelvlakken, daar waar de ene partij denkt bepaalde zaken wel te hebben uitbesteed, terwijl de andere partij denkt van niet. Daar ontstaat ruis. Hoe duidelijker de koppelvlakken zijn – technisch, organisatorisch en wat betreft verantwoordelijkheden – hoe beter je ‘in control’ bent en hoe beter je dus ook je verantwoordelijkheden kunt nakomen.

Onderscheidend

De wet bescherming persoonsgegevens stelde al zware eisen aan de beveiliging van persoonsgegevens. De nieuwe Wet meldplicht datalekken stimuleert organisaties om nog eens heel goed na te denken over welke informatie ze daadwerkelijk willen opslaan, omdat dit een serieuze verantwoordelijkheid én aansprakelijkheid met zich meebrengt. Het lastige is dat nog moet blijken hoe de wet in de praktijk zal uitpakken en hoe de Autoriteit Persoonsgegevens zal optreden bij grote incidenten. Kuper en Voskamp zijn niettemin positief over de functionaliteit van de wet en zien voor accountantskantoren en SRA kansen. “Het zou goed zijn als SRA-leden met elkaar een norm voor informatiebeveiliging afspreken waaraan iedereen minimaal moet voldoen”, aldus Voskamp. “Iets dergelijks bestaat bijvoorbeeld al voor gemeenten en die hebben er veel voordeel van.”

Ook voor individuele kantoren liggen er mogelijkheden, vindt Kuper. “Accountants worden door hun klanten steeds meer gezien als ‘financiële huisarts’. De rol als sparringpartner op het gebied van informatiebeveiligingsvraagstukken sluit naadloos aan op deze rol en is een uitgelezen kans om je als accountantskantoor als innovatief te profileren. Wij zien dat een aantal SRA-kantoren dat ook echt doet. Zij hebben zich verdiept in de wetgeving en gaan er bewust mee om richting klanten, om hen te behoeden voor calamiteiten. Wij hopen dat meer kantoren dit initiatief zullen volgen.”

Masterclass Strategie

Tijdens vier bijeenkomsten gaan topsprekers en bestuurders van middelgrote SRA-kantoren in gesprek over verschillende strategische onderwerpen.

Kijk op www.sra.nl voor meer informatie of mail uw vragen naar masterclass@sra.nl.