ik wil mobiel werken



De businesscase van goede security: overtuig je directie

in samenwerking met

Wil je als IT-manager graag genoeg geld en aandacht voor security binnen je bedrijf, maar weet je niet goed hoe je dit aan moet pakken? Er zit vaak een verschil tussen de manier waarop directies en IT- en securitymanagers denken en werken. In dit document lees je hoe je de directie kunt overtuigen met een ijzersterke businesscase.

‘Geen moetje, maar zakelijke kansen’

Pelle Aardewerk is securityexpert bij HP, hij komt regelmatig bij organisaties over de vloer om hen te helpen hun beveiliging naar een hoger niveau te tillen. Voordat hij bij HP aan de slag ging, heeft hij voor verschillende corporates businesscases gemaakt om directies te overtuigen dat security zakelijke kansen biedt. “Directies moeten keuzes maken hoe ze geld besteden”, vertelt Aardewerk. “Hoeveel je precies uit moet geven aan security is lastig te kwantificeren. Er gebeurt ontzettend veel in de markt, dus het is niet voldoende om simpelweg 5% meer dan vorig jaar te begroten.”

Het lastige is echter dat directie en IT vaak totaal anders denken over prioriteiten. “Hoe overtuig je de directie dan dat security niet zomaar een ‘moetje’ is, maar echt zakelijke kansen biedt? Dat doe je met een businesscase.”

Stap 1: Laat je businesscase aansluiten bij de doelstellingen

Van de honderd risico’s binnen een organisatie is er vaak maar geld en resources om twintig echt belangrijke te managen. Maar hoe wordt security dan een prioriteit? “Het is voor directies ontzettend belangrijk dat een businesscase gelinkt is aan de belangrijkste doelstellingen van een organisatie. Hiervoor breng je allereerst de beslissers in de organisatie in kaart. Wie is er verantwoordelijk en wie gaat er betalen? Denk hierbij bijvoorbeeld aan een CIO, CFO of CISO. Je moet heel goed inspelen op wat de directie belangrijk vindt. Zijn customer experience, medewerkersproductiviteit en beschikbaarheid

Wanneer je een businesscase gaat schrijven, doe je dat het beste met behulp van de **5 W's en 1 H**

W	W	W	W	W	H
waarom	wat	wie	waar	wanneer	hoe

van bedrijfskritische systemen bijvoorbeeld heel belangrijk, maar is mijn businesscase daar niet aan gelinkt? Dan wordt het geen prioriteit voor de directie. Je moet bij die top 20 komen."



Stap 2: beschrijf de 5 w's en 1 h in je businesscase

Wanneer je een businesscase gaat schrijven, doe je dat volgens Aardewerk het beste met behulp van de 5 w's en 1 h: waarom, wat, wie, waar, wanneer en hoe. "Vooral waarom en wat zijn heel belangrijk. Je vertelt waarom je het geld nodig hebt, en hoe het helpt om de bedrijfsdoelstellingen te behalen. Vervolgens beschrijf je wat je exact gaat doen."

"Om de emotie eruit te halen, kun je het beste drie alternatieven geven. Van elk van deze mogelijkheden geef je aan wat de gevolgen van dat besluit zijn voor de organisatie", vertelt Aardewerk. Door de scenario's te vergelijken geef je de directie een helder beeld van de voor- én nadelen en de impact per optie.

Hij adviseert om ook de mogelijkheid dat de organisatie géén extra budget besteedt aan security op te nemen in je businesscase. "Maar dan moet je ook duidelijk maken wat de risico's zijn en de impact is van die keuze. Wanneer er niet genoeg middelen zijn voor het beschermen van de organisatie, is de kans op een impactvolle securityaanval aanzienlijk groter dan wanneer dit er wel is. Dat kan veel klanten en geld kosten, en productiviteitsverlies veroorzaken. Als IT- en securityafdeling ben je verantwoordelijk voor eventuele cyberaanvallen. Wanneer je deze risico's vastlegt in de businesscase, kun je in geval van crisis altijd aantonen dat je deze in het vizier had."



Stap 3: Schrijf een *note for decision*

Als je een directie wilt overtuigen meer budget en middelen vrij te maken voor security, is het slim om vòòr de vergadering al een document met informatie rond te sturen. "Ik schreef altijd een note for decision van maximaal drie pagina's, waarin ik beschreef wat de plannen waren én waarom. Ook gaf ik verschillende alternatieven."

Door zo'n document op te stellen, zorg je ervoor dat de directie al weet waar je plannen over gaan en hoe toekomstige waardevolle data en systemen tot een acceptabel niveau worden beschermd. Met deze voorkennis is de kans groter dat er daadwerkelijk een weloverwogen kwalitatieve keuze wordt gemaakt tijdens de vergadering.



Stap 4: Organiseer een *premeeting*

Volgens Pelle is 'geen besluit' het slechtste scenario wanneer het gaat om meetings over securitybudget. Daarom pleit hij naast een tijdige note for decision ook voor een *premeeting* waarbij je als IT- of securitymanager één-op-één spreekt met de belangrijkste beslissers. "Wanneer zij de note for decision hebben gelezen, komen ze met allerlei vragen. Door deze alvast te beantwoorden, en je uitgewerkte businesscase en presentatie waar nodig aan te passen, maak je de weg vrij voor een besluit tijdens de uiteindelijke vergadering. Ook begrijp je door zo'n *premeeting* beter welke politieke agenda elk directielid heeft."

De grootste security-uitdagingen richting 2030

De risico's die nu bovenaan de agenda staan, zijn nog maar het begin. Technologische ontwikkelingen gaan razendsnel, en de dreigingen die organisaties richting 2030 te wachten staan, vragen nú om aandacht. Wie pas reageert als een dreiging actueel is, is te laat.

1.

AI als wapen én schild

Kunstmatige intelligentie verandert het speelveld fundamenteel, aan beide kanten van de scheidslijn. AI stelt beveiligingsteams in staat om bedreigingen in real-time te detecteren en te neutraliseren, maar cybercriminelen maken er inmiddels ook gebruik van: ze bouwen er phishing-aanvallen mee die nauwelijks van echte communicatie te onderscheiden zijn. Richting 2030 wordt dit onderscheid alleen maar moeilijker te maken.

2.

De kwantumdreiging: nu voorbereiden

Quantumcomputing staat al in de top 10 van de meeste lijstjes met huidige risico's, maar de urgentie neemt de komende jaren alleen maar toe. Quantumcomputers worden in staat geacht om de meest gebruikte vormen van encryptie te kraken. En dat is al een uitdaging, omdat versleutelde informatie die nu wordt onderschept later alsnog ontcijferd kan worden door een quantumcomputer.

Organisaties die wachten tot quantumcomputing mainstream is, zijn dan te laat. De migratie naar post-quantum cryptografie vraagt om bewustwording op directieniveau én voldoende middelen. Breng in kaart waar cryptografie binnen je organisatie wordt toegepast, in bibliotheken, IoT-apparaten, communicatieprotocollen, opslagsystemen en databases.

3.

Tekort aan security-professionals

Het tekort aan cybersecurity-professionals is één van de belangrijkste uitdagingen richting 2030, naast de risico's van menselijke fouten en verouderde systemen. Beveiligingsteams worden geconfronteerd met toenemende complexiteit, terwijl het moeilijker blijft om expertise vast te houden en continuïteit te waarborgen. Het wordt daarom nóg belangrijker om te investeren in opleidingen en kennisbehoud.

4.

Van verdediging naar weerbaarheid

De rode draad door al deze uitdagingen is een fundamentele verschuiving in de mindset. Cybersecurity wordt steeds minder een kwestie van het verdedigen van vestingen, en steeds meer van het accepteren van voortdurend cyberrisico, met als belangrijke focus het vergroten van weerbaarheid en het vermogen om snel te herstellen.

Stap 5: Knopen doorhakken tijdens de meeting

Wanneer je vervolgens de vergadering met alle beslissers ingaat, is iedereen al op de hoogte van de belangrijkste punten. “Het is dan nuttig om één of twee aanvullende slides met highlights uit de note for decision te presenteren, zodat iedereen gevoelsmatig klaar is om een besluit te nemen. Vervolgens licht je de cost/benefits uit: wat kost elke keuze en wat levert het concreet op voor de organisatie? Hierbij is het belangrijk om te benadrukken dat er niet alleen aanschafkosten zijn, maar dat er gedurende de gehele levens-cyclus kosten komen. Denk bijvoorbeeld aan onderhoudskosten.”

Wanneer er aan het einde van de vergadering een knoop wordt doorgehakt, is het tijd om een verantwoordelijke voor het project te benoemen. Wie heeft de leiding tijdens de implementatie? “Meestal is dit de IT- en securitymanager. Ook is het nuttig een steering committee te benoemen met vertegenwoordigers vanuit de Business, IT en Security. Wanneer er wordt gekozen voor een oplossing waar eindgebruikers mee moeten gaan werken, is het ook belangrijk om een business change manager aan te wijzen. Die gaat ervoor zorgen dat de nieuwe oplossing daadwerkelijk wordt gebruikt.

“Vaak duurt het zes tot twaalf maanden voordat een oplossing optimaal kan worden ingezet en de beoogde doelstellingen worden behaald. Dat is het moment dat de verantwoorde-lijkheid over gaat van de IT-manager naar de business change manager. Dit zijn verschil-lende verantwoordelijkheden met eigen KPI’s.”

Stap 6: Presenteer je businesscase na een tijdje opnieuw

Kiest de directie ervoor om niets te doen, of maar een deel van de adviezen op te volgen? Dan is het altijd een optie om later terug te komen op je businesscase en deze gereviseerd te presenteren. “Situaties en risico’s veranderen over tijd. Soms wordt de impact van een bepaald risico ook groter. Dan is de directie wellicht meer bereid om budget vrij te maken.”

Het lijkt misschien veel werk om een uitge-breide businesscase op te zetten om je directie te overtuigen. Toch is dit het volgens Aardwerk meer dan waard. “Je maakt namelijk glashelder en onderbouwd duidelijk waarom extra budget noodzakelijk is, zonder dat dit overkomt als ‘zeuren’. De kans is groter dat je daadwerkelijk extra geld, materiaal en mankracht toegewezen krijgt. Hierdoor kun je security-beleid uitrollen dat je organisatie futureproof maakt.”

Cyberaanvallen wachten nóóit op een goed moment. HP Wolf Security beschermt je organisatie op hardwareniveau, van endpoints tot printers, zodat jouw mensen veilig kunnen werken, waar ze ook zijn. Minder waarschuwingen, minder herstelwerk, meer controle. Vraag een vrijblijvende demo aan.