Microsoft Security

De kosten van inactiviteit

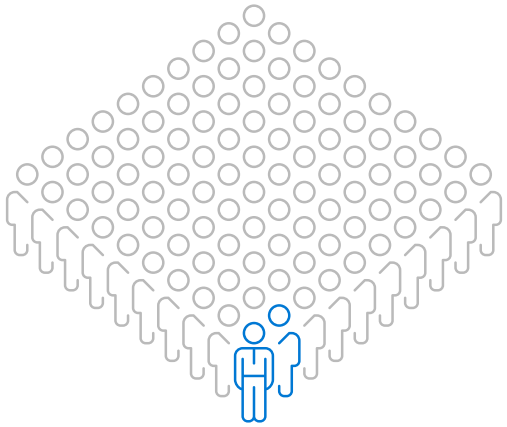
Hoe overtuig je als CISO de raad van bestuur van de noodzaak om te investeren in cybersecurity

Als CISO begrijp je als geen ander de securityrisico's waarmee jouw organisatie te maken heeft. Jij hebt de technische expertise, je bent op de hoogte van de huidige bedreigingen en je weet hoe gevaarlijk deze zijn voor de zwakke plekken van je organisatie. En je bent je er terdege van bewust dat de gemiddelde kosten van een lek blijven stijgen, tot een ongekend hoogtepunt van USD 4,35 miljoen in 2022.

Je weet echter ook hoe deze risico's in bredere zakelijke trend passen. Je hebt geleerd hoe je moet werken bij economische onzekerheid, onder de druk om meer te doen met minder en met een tekort aan talent, waardoor jij gedwongen werd om je steeds verder te blijven ontwikkelen.

Te midden van al deze uitdagingen heeft cybersecurity een nieuwe urgentie gekregen, zelfs bij de raad van bestuur. Als gevolg hiervan hebben CISO's een bredere toegang en invloed gekregen in organisaties (waarbij sommigen zelfs de rol van CIO hebben overgenomen). Veel van hen staan onder druk om de noodzaak van investeringen in cybersecurity rechtstreeks aan te kaarten bij hun bestuur. Hoe kom je dan goed beslagen ten ijs?

Je bestuursraad heeft de macht om prioriteiten te stellen die de security van je organisatie een veilige basis geven. Maar gemiddeld heeft nog geen 2 procent van de leden van een raad van bestuur relevante, recente ervaring in cybersecurity En veel bestuursleden hebben geen goed overzicht over IT en security, of ze hebben een ambivalente visie op de rol van de raad met betrekking tot security.



Gemiddeld heeft minder dan 2 procent van de leden van een raad van bestuur relevante, recente ervaring in cybersecurity.

Gelukkig is er bij de meeste besturen wel een enorm potentieel om steun te krijgen voor investeringen in security. De topprioriteiten van een gemiddelde raad hebben te maken met risico, reputatie en financiële stabiliteit. En die factoren zijn onlosmakelijk verbonden met een goede security.

Als je het verband tussen deze prioriteiten en de securityresultaten duidelijk kunt maken, ben je goed op weg om een sterke, ROI-gerichte pitch te maken. Deze gids helpt je de juiste context en aanpak te ontwikkelen en laat zien hoe je het volgende doet:

- **Denken als een bestuurslid**
- **Spreken als een bestuurslid**
- **Voorbeelden uit de praktijk gebruiken om risico's concreet en relevant te maken**

Denken als een bestuurslid

Wellicht is je bestuur meer bezig met security dan jij denkt.

Security komt nu vaker dan ooit aan de orde in vergaderingen van de raad. Meer dan tweederde van de bestuursraden zegt dat cybersecurity regelmatig of voortdurend gespreksonderwerp is en 77 procent van de bestuurders is van mening dat cybersecurity een topprioriteit is voor hun raad. En hoewel bestuurders over het algemeen weinig ervaring hebben met cybersecurity, hebben ze dat steeds vaker wel met algemene technologie. Bij toonaangevende bedrijven heeft 79 procent van de raden ten minste één lid met een technologische achtergrond, en bij 72 procent van die bedrijven hebben technologieleiders vaak buiten bestuursvergaderingen om contact met het bestuur.

Dat is allemaal veelbelovend voor CISO's. Het is echter nog steeds raadzaam om minder te praten over technologie en meer over het grotere geheel van bedrijfsrisico- en reputatiebeheer. Alle bestuurders kunnen ongeacht hun technische expertise zonder problemen meepraten en nadenken over risico's, of het nu gaat om het vinden van de juiste mate van risicotolerantie of het evalueren van risicobeheerplannen.

> **Cybersecurity gaat over het nemen van de juiste risico's, niet over het kiezen van de juiste technologie."**

Probeer je in te leven in de mindset van je bestuur en begin met het bouwen van consensus over de huidige status van je organisatie:

- **Wat zien bestuursleden als je belangrijkste assets? Zijn dat je klantdata, het intellectuele eigendom van het bedrijf, je merk of iets anders?**
- **Wat zien zij als de meest bedreigende risico's?**
- **Wat zijn de belangrijkste prioriteiten van de organisatie?**
- **Welke doelstellingen moet het bedrijf bereiken en hoe kan jouw securityprogramma deze helpen realiseren?**

Door dit als uitgangspunt te gebruiken voor het gesprek, ontstaat het juiste perspectief. Je kunt benadrukken dat cybersecurity gaat over het nemen van de juiste risico's, niet over het kiezen van de juiste technologie.

Spreken als een bestuurslid

Houd de volgende ideeën in gedachten terwijl je praat met je bestuur, of dat nu in presentaties of minder formele communicatie is.

Praat over zaken, niet over technologie.

Gebruik voorbeelden en illustraties die geschikt zijn voor geïnteresseerde zakelijke experts, geen technische experts. Gebruik Bloomberg Businessweek of The Wall Street Journal als inspiratiebron voor het juiste detailniveau om securityconcepten te presenteren. (Een recent nieuwsbericht over een datalek kan ook een goed uitgangspunt voor het gesprek zijn, omdat je aan de hand hiervan kunt beschrijven hoe dat in je eigen bedrijf had kunnen uitpakken.) Zoek iemand buiten je security-organisatie die je vertrouwt en die je feedback kan geven op de complexiteit van je communicatie.

Presenteer jezelf als een onafhankelijke gids en facilitator.

Voor een goed securityprogramma moet je het juiste evenwicht zien te vinden. Dat betekent dat er een acceptabel risiconiveau moet zijn om bedrijfsdoelstellingen na te streven. Jij kunt helpen die mindset te bevorderen. Maak aan bestuurders duidelijk welke afwegingen er spelen en begeleid ze bij beslissingen in plaats van als een autoriteit oplossingen voor te schrijven.

Richt je op de ROI, vooral wat de strategische relevantie betreft.

Laat altijd zien hoe je security-initiatieven aansluiten bij zakelijke behoeften en prioriteiten op de lange termijn. Ga uit van de belangrijkste strategische doelen van je organisatie, of het nu gaat om wereldwijde uitbreiding, een nieuw klantenplatform of digitale transformatie, en bied de context die laat zien hoe de juiste investeringen in cybersecurity deze doelen mogelijk maken en beschermen.

> **Maak aan bestuurders duidelijk welke afwegingen er spelen en begeleid ze bij beslissingen in plaats van als een autoriteit oplossingen voor te schrijven."**

Focus op kansen, niet op kosten.

Security (en IT in bredere zin) kan worden gezien als niets meer dan een noodzakelijke kostenpost. Je kunt je team dan blijven pushen om manieren te vinden om proactiever te zijn. Je kunt je echter ook meer richten op de rol die security als zakelijke factor kan spelen. Als je als CISO kunt aantonen hoe security de omzet kan verhogen, bijvoorbeeld door contract- en klantwaarde te kwantificeren tegenover de uitgaven voor controles, zul je waarschijnlijk een ontvankelijker publiek vinden.

Wees voorbereid met metrics en benchmarks.

"Wat je niet kunt meten kun je niet verbeteren" is misschien wat kort door de bocht, maar zorgvuldig opgestelde metrics kunnen nog steeds een krachtig bewijs vormen voor bestuurders. Kies metrics die de maturiteit en de voortgang van het programma in de loop van de tijd aantonen (zoals metrics over training in securitybewustzijn of de effectiviteit van securityprocedures) en die laten zien hoe je organisatie het doet ten opzichte van collega's. Deze maturiteitsmetrics zullen voor bestuurders over het algemeen zinvoller (en bruikbaarder) zijn dan metrics over prestaties of activiteit, die vaak meer ruis bevatten en een technischere context vereisen. Metrics kunnen je ook helpen bij het aantonen van de ROI en verstandige budgettering. Het is bijvoorbeeld raadzaam om goed in de gaten te houden of je evenredige uitgaven op verschillende securitygebieden ongeveer op dezelfde lijn liggen als die van vergelijkbare organisaties.[1]

Beschrijf risico's op manieren die ze concreet maken.

Te veel nadruk leggen op angst is meestal niet de beste weg naar steun en positieve actie. Het juiste voorbeeld of incident uit de praktijk kan daarentegen uiterst effectief zijn om de complexiteit en het risico over te brengen, zonder overdrijving of negativiteit. Zoek naar specifieke voorbeelden die relevant zijn voor jouw branche of organisatie, of die reële scenario's illustreren, zoals insiderrisico's of ransomware. (Zie het volgende gedeelte voor ideeën.)

[1] Planning Guide 2023: Security & Risk, Forrester, 2023

Voorbeelden uit de praktijk gebruiken om risico's concreet en relevant te maken

Insiderrisico's en ransomwareaanvallen blijven belangrijke bedreigingen voor veel organisaties. Dit zijn dan ook nuttige voorbeelden om tastbare, concrete risico's te illustreren. Door incidenten uit de praktijk te beschrijven aan bestuurders, kun je ze een beter inzicht geven in dit soort aanvallen, de mogelijke gevolgen ervan en welke investeringen in cybersecurity een oplossing kunnen bieden bij soortgelijke aanvallen in de toekomst.

Voorbeeld van een ransomware-incident:

LockerGoga-aanval

Maart 2019

Wat is er gebeurd?

Een van de grootste aluminiumbedrijven ter wereld werd aangevallen met LockerGoga, een vorm van ransomware. Door de aanval werden de bestanden op duizenden servers en pc's vergrendeld. Op het scherm van de getroffen computers verscheen een losgeldeis. De aanval werd drie maanden eerder in gang gezet toen een werknemer nietsvermoedend een geïnfecteerde e-mail van een vertrouwde klant opende. Hierdoor konden hackers de IT-infrastructuur binnendringen en hun virus heimelijk planten.

Wat was de impact op het bedrijf?

Alle 35.000 werknemers van de organisatie in 40 landen werden getroffen. In sommige van de 170 fabrieken werden productielijnen gestopt. Andere faciliteiten stapten over van computergestuurde naar handmatige activiteiten. De financiële impact bedroeg uiteindelijk USD 71 miljoen.

Wat zou er anders gedaan kunnen worden om soortgelijke aanvallen in de toekomst te voorkomen?

De snelle en transparante reactie van het bedrijf werd alom geprezen. Ze kozen ervoor om geen losgeld te betalen, volledig open te zijn over de inbreuk en de hulp in te roepen van het Detection and Respons Team van Microsoft (DART), dat bedrijven ondersteunt die te maken hebben met een aanval. Om soortgelijke aanvallen in de toekomst te voorkomen, schetsten DART-leden het belang van de juiste combinatie van mensen, processen en technologie. Dit omvat de implementatie van meervoudige verificatie, een gedegen updateproces, back-ups van data en het vergroten van het securitybewustzijn met bijbehorende training van werknemers.

De case formuleren

De ideeën en voorbeelden die in dit eBook worden besproken, kunnen je helpen je pitch voor de raad van bestuur vorm te geven. Uiteindelijk moet je natuurlijk de juiste structuur en details kiezen op basis van de investeringen die je nodig hebt. Aan de hand van de volgende ideeën kun je onderzoeken wat het beste werkt voor jouw specifieke bestuur.

- **Wees niet bang om verschillende benaderingen uit te proberen.** Simulaties kunnen bijvoorbeeld heel nuttig zijn voor voorlichting en betrokkenheid. Of je kunt een externe security-expert als spreker inschakelen.
- **Praat met collega's uit het topmanagement voor feedback en support.** Je CEO en andere collega-managers kunnen je belangrijke inzichten geven over bepaalde bestuursleden of terugkerende problemen. Jouw argumenten krijgen ook extra gewicht als bestuurders zien dat managers in je organisatie de investeringen ondersteunen die jij voorstelt.
- **Houd de communicatielijnen open.** Probeer met een of meer bestuurders een band op te bouwen buiten de driemaandelijkse of jaarlijkse updates, met name bestuurders die ervaring hebben met technologie of security. Zij kunnen helpen bij het verdedigen van je standpunten als jij er niet bij bent en ze kunnen je zelfs helpen je pitch beter af te stemmen.

Uiteindelijk hebben CISO's nu veel reden om vertrouwen te hebben. Meer bestuurders dan ooit zijn actief op zoek naar advies over cybersecurity. En veel technologische ontwikkelingen sluiten rechtstreeks aan bij de zorgen over kosten en de ROI van bestuurders. Denk bijvoorbeeld aan de vooruitgang in automatisering en AI, of de mogelijkheden die geïntegreerde security-oplossingen bieden om de complexiteit en kosten terug te dringen.

Waar moet je beginnen?

Gebruik de volgende discussiegids om te bedenken hoe de SecOps-maturiteit je kan helpen een gesprek met bestuurders vorm te geven.

Maturiteit van SecOps gebruiken om een gesprek te starten met je bestuurders

Hoe begin je een gesprek met bestuurders over cybersecurityrisico's? De maturiteit van security-activiteiten kan je een kader bieden voor productievere gesprekken.

Neem de tijd om de volgende vijf SecOps-gebieden te bespreken met je team van securitymanagers. Als je meer inzicht hebt in waar jouw organisatie zich in het maturiteitsspectrum voor elk gebied bevindt, kun je hiaten en sterke punten identificeren. Aan de hand van die kennis kun je vervolgens met specifiekere verzoeken komen bij je raad van bestuur.

Een organisatie die zich voor Triage bijvoorbeeld aan het Basis-uiteinde van het spectrum bevindt, gebruikt misschien nog geen automatisering om incidenten met een hoog volume of herhalende incidenten te onderzoeken en verhelpen. Een organisatie die daarentegen Geoptimaliseerd is voor Triage, gebruikt bijvoorbeeld SOAR-services en -tools (Security Orchestration, Automation and Response) om de preventie van cyberaanvallen en de reactie hierop te automatiseren. Door terug te keren naar het idee van acceptabel risico rond verschillende bedreigingen, kun je het bestuur helpen beter te bepalen waar je organisatie zich in dat continuüm moet bevinden.

Bekijk de volledige zelfevaluatietool voor meer informatie.

Triage

Hoe snel kunnen we waarschuwingen beoordelen, prioriteiten stellen en incidenten naar ons Security Operations Center doorsturen om op te lossen?

Discussievragen voor je securitymanagementteam:

- Hebben we de juiste aanpak om incidenten en bedreigingswaarschuwingen te prioriteren?
- Moeten we meer automatisering gebruiken om incidenten met een hoog volume of herhalende incidenten te onderzoeken en op te lossen?
- Doen we genoeg om meldingsmoeheid te beheersen?

Onderzoek

Hoe snel kunnen we bepalen of een waarschuwing betrekking heeft op een werkelijke aanval of een vals alarm is?

Discussievragen voor je securitymanagementteam:

- Hoeveel securitytools gebruiken onze analisten in totaal om incidenten te onderzoeken (inclusief producten of portals van leveranciers en aangepaste tools of scripts)?
- Hoe consolideren en correleren we al onze databronnen (bijvoorbeeld met een SIEM-tool of andere tools)?
- Hoe gebruiken we detectie- en onderzoekstools die zijn gericht op identiteit, eindpunten, e-mail en data, SaaS-apps of cloudinfrastructuur?

Opsporing

Hoe sporen we tegenstanders op die aan onze primaire en geautomatiseerde verdediging zijn ontsnapt?

Discussievragen voor je securitymanagementteam:

- Moet proactief opsporen van bedreigingen een groter deel uitmaken van onze securitystrategie?
- Hebben we de juiste processen en tools om bedreigingen van binnenuit te detecteren en beheren?
- Besteedt ons opsporingsteam voldoende tijd aan het verfijnen van waarschuwingen zodat triageteams meer true positives krijgen?

Incidentbeheer

Hoe coördineren we de respons door technische, operationele, communicatie-, juridische en governancefuncties?

Discussievragen voor je securitymanagementteam:

- Hebben we een effectief crisisbeheersingsproces voor de afhandeling van grote security-incidenten?
- Zijn bij het proces de juiste teams betrokken, inclusief het uitvoerend management, juridische zaken, en communicatie en PR?
- Houden we vaak genoeg regelmatige oefeningen om dit proces te trainen en te verfijnen?

Automatisering

Hoe zetten we automatisering in om tijd te besparen voor onze analisten, de reactiesnelheid te verhogen en de workloads terug te dringen?

Discussievragen voor je securitymanagementteam:

- Hoe gebruiken we door leveranciers geleverde of onderhouden automatisering om de workload van analisten voor onderzoek en herstel te verkleinen?
- Hoe goed kunnen we geautomatiseerde acties voor verschillende tools orkestreren?
- Maken we gebruik van automatisering die door de community wordt geleverd?

Microsoft Security