HANDLEIDING CEO-NIVEAU: LEIDERSCHAP IN CYBERBEVEILIGING

BESTUUR

De cyberbeveiliging van uw organisatie staat of valt met het hoogste managementniveau. De CEO moet samen met de raad van bestuur de risico's begrijpen en de eindverantwoordelijkheid nemen voor de cyberbeveiligingsactiviteiten en -medewerkers in de organisatie. U moet:

- Een centrale informatiebeveiligingsfunctionaris (chief information security officer [CISO]) aanwijzen indien dit nog niet gebeurd is of, als de middelen hiervoor niet toereikend zijn, iemand binnen uw organisatie aanwijzen om de rol van CISO op zich te nemen.
- Samenwerken met de CISO of ander technisch personeel om een cyberbeveiligingsstrategie en -kader op te stellen en toe te passen die is afgestemd op de specifieke cyberrisico's van de organisatie op basis van internationale, nationale en industrienormen en -richtlijnen.
- Duidelijke rollen en verantwoordelijkheden formuleren voor medewerkers die de cyberbeveiliging van de organisatie implementeren en beheren.
  - Samenwerken met de CISO om de juiste cyberbeveiligingsrollen en toegangsrechten voor alle personeelsniveaus vast te stellen.
  - In goede banen leiden van communicatie en samenwerking om ervoor te zorgen dat cyberbeveiligingsmanagement holistisch is, vooral als verantwoordelijkheden op het gebied van cyberbeveiliging worden gedeeld door meerdere medewerkers of divisies binnen de organisatie (zoals het hebben van aparte verticale structuren voor informatiebeveiliging, risico's en technologie).
- Ervoor zorgen dat de CISO weet bij wie hij moet zijn om u en de raad van bestuur tijdig op de hoogte te brengen van bedreigingen.
- De CISO of ander technisch personeel vragen om het senior management geregeld te briefen.
- Ervoor zorgen dat het beveiligingsbeleid, de normen, handhavingsmechanismen en procedures van de organisatie uniform zijn in alle teams en bedrijfsonderdelen.

RISICOBEOORDELING EN -BEHEER

Om te zorgen voor een sterk bewustzijn van cyberbeveiliging en voorbereid zijn voor als het misgaat, moeten risico's continu geanalyseerd worden. De cyberbeveiliging van uw organisatie kan worden verbeterd door:

- Risicobeoordeling en beheer van cyberbeveiliging als prioriteit vast te stellen binnen de bredere risicobeheer- en bestuursprocessen van uw organisatie. Samen te werken met uw CISO of ander technisch personeel aan een plan voor uitvoering van een risicobeoordeling die het volgende omvat:
  - Beschrijven van de activa van uw organisatie en de mate waarin deze afhankelijk zijn van technologie,
  - Beoordelen van de volwassenheid van uw organisatie en de inherente risico's die aan de technologische afhankelijkheid van haar activa kleven,
  - Bepalen van de gewenste volwassenheid van uw organisatie,
  - Begrijpen waar cyberdreigingen in de lijst met risicoprioriteiten van uw organisatie staan,
  - Vaststellen in hoeverre uw huidige cyberbeveiligingsstatus overeenkomt met de gewenste doelstatus,
  - Implementeren van plannen om volwassenheid te bereiken en in stand te houden,
  - Evalueren en oormerken van fondsen om in veiligheid te investeren en bestaande hiaten aan te pakken.
  - Voortdurend opnieuw evalueren van de volwassenheid, risico's en doelen van uw organisatie op het vlak van cyberbeveiliging, en
  - Overwegen om derden penetratietesten of 'red teaming-oefeningen' te laten uitvoeren,
  - Overwegen om beveiligingsmaatregelen te nemen, zoals de aanschaf van een cyberverzekering.
- De inspanningen van werknemers tijdens het risicobeoordelingsproces te kanaliseren om ervoor te zorgen dat de organisatie snel kan reageren.
- De resultaten van de risicobeoordeling te analyseren en presenteren zodat het management, maar ook de belangrijke stakeholders en de raad van bestuur, toezicht kunnen uitoefenen.
- Houd toezicht op alle veranderingen zodat de organisatie zoals gewenst of adequater kan reageren op cyberdreigingen, inclusief adequaat budgetbeheer, waarbij alle maatregelen die worden genomen om de cyberbeveiliging te verbeteren afgestemd moeten zijn op de risico's en betaalbaar moeten zijn voor uw organisatie.
- Toe te zien op de effectiviteit van continue monitoring om slagvaardig en flexibel te kunnen blijven reageren op cyberrisico's die zich voordoen.

ORGANISATIECULTUUR

De cyberbeveiliging van uw organisatie is geen eenmalige klus die door een handjevol medewerkers geklaard kan worden; het is een factor om rekening mee te houden bij alle zakelijke beslissingen en activiteiten en iets waar alle medewerkers een rol in blijven spelen. Doe het volgende om ervoor te zorgen dat de cyberbeveiliging door de hele organisatie heen continu op peil blijft:

- Voer cyberbeveiligingsgesprekken met het leiderschapsteam en communiceer regelmatig met het personeel dat verantwoordelijk is voor het beheer van cyberrisico's.
- Geef alle nieuwe medewerkers een cyberbeveiligingstraining, zorg ervoor dat alle medewerkers op de hoogte zijn van het cyberbeveiligingsbeleid van uw organisatie – en laat ze documenten ondertekenen waarin ze toezeggen dit beleid na te leven – en zorg ervoor dat uw IT-afdeling of ander technisch personeel hen heeft ingelicht over best practices.
- Laat alle medewerkers periodiek cyberbeveiligingstrainingen volgen met betrekking tot hun beveiligingsverantwoordelijkheden op korte en lange termijn.
- Zorg ervoor dat uw organisatie cyberbeveiliging altijd laat meewegen bij de keuze van potentiële leveranciers en het delen van gegevens met derden.
- Integreer een beoordeling van de cyberbeveiliging van een organisatie bij het overwegen van fusies en overnames.
- Beoordeel jaarlijks het cyberbeveiligingsbeleid van uw organisatie.
- Stimuleer de vrijwillige informatie-uitwisseling over cyberdreigingen en incidenten binnen uw organisatie en met betrouwbare concurrenten.
- Bevorder innovatie die vanaf het begin rekening houdt met beveiligingsproblemen en -planning.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE
INTERNATIONAL MONETARY FUND · THE WORLD BANK IBRD • IDA | WORLD BANK GROUP · SWIFT · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE · ICBA Independent Community Bankers of America®