ISO 27001:2022 & Peakproteqt MDR

Acht controles uit bijlage A die technische diepgang vragen en hoe onze Managed Detection & Response-dienst die voor jou invult, van logging tot aan incident response.

A.8.15 · LOGGING

Organisaties moeten logs aanmaken, bewaren en beschermen van activiteiten in systemen, denk aan inlogpogingen, toegang tot gevoelige data, systeemwijzigingen. Logs mogen niet aangepast of verwijderd kunnen worden door onbevoegden.

Peakproteqt: Wij richten, bewaren en beschermen, door middel van ons SIEM, de logging centraal in. Elke inlogpoging en wijziging op ons eigen SIEM-platform controleren wij, om zo de integriteit en vertrouwelijkheid van de data te behouden. Door sterke authenticatie kunnen onbevoegde niet zomaar bij de data. Bij twijfel kan de klant altijd een audit rapport opvragen.

A.8.16 · MONITORING

Netwerken, systemen en applicaties moeten actief bewaakt worden op afwijkend gedrag. Er moeten procedures zijn om anomalieën te herkennen en op te volgen.

Peakproteqt: Onze MDR-oplossing bewaakt continue jouw netwerk, applicaties en systemen op afwijkend gedrag. Indien afwijkend gedrag wordt gedetecteerd krijgt ons SOC hier een melding van, zodat we hier direct opvolging aan kunnen geven. Wij zorgen er daarnaast voor dat je als bedrijf altijd meebeweegt met het dreigingslandschap.

A.5.24 · INCIDENT PLANNING

Er moet een gedocumenteerd proces zijn voor het managen van informatiebeveiligingsincidenten, inclusief rollen, verantwoordelijkheden en escalatiepaden. Dit moet vóór een incident op orde zijn, niet erna.

Peakproteqt: Binnen Peakproteqt hebben we incident response plannen klaarliggen om adequaat op cyberdreigingen te kunnen acteren. Daarnaast krijgen al onze klanten een incident response plan, zodat ook zij weten wie ze moeten bellen en wie waar verantwoordelijk voor is. Beter vooraf goed plannen dan achteraf chaotisch rondrennen.

A.5.25 · BEOORDELING

Niet elk event is een incident. De norm vraagt dat organisaties kunnen beoordelen of een gemelde gebeurtenis daadwerkelijk een informatiebeveiligingsincident is, en dat dit op basis van criteria gebeurt.

Peakproteqt: Niet elke gebeurtenis binnen jouw systemen of applicaties is direct een dreiging. Denk aan een IT-beheerder die jullie servers onderhoud. Als deze gebeurtenis voorkomt, classificeren wij de melding, doen onderzoek en oordelen of dit daadwerkelijk een cyber incident is. Dit gebeurt allemaal achter de schermen, zodat onze klanten hier geen omkijken naar hebben. Ons incident classificatieproces is gestandaardiseerd en gedocumenteerd.

A.5.26 · RESPONSE

Bij een incident moet er een gestructureerde respons zijn: beheersen, onderzoeken, communiceren en herstellen. Dit moet gedocumenteerd en reproduceerbaar zijn.

Peakproteqt: Onze MDR-dienstverlening bevat standaard incident response, zodat wij er direct voor onze klanten zijn wanneer dit het hardst nodig is. Indien we een cyberaanval detecteren in jouw systeem, handelen we daar direct naar door bijvoorbeeld systemen te isoleren, malware te verwijderen en gebruikers te blokkeren. De genomen acties en het proces wordt allemaal beschreven, zodat terug te lezen is hoe wij hebben gehandeld.

A.5.27 · LEREN

Na een incident moet de organisatie aantonen dat zij ervan geleerd heeft: wat ging er mis, wat kan beter, en zijn verbeteringen doorgevoerd?

Peakproteqt: Aansluitend op control A5.26, kunnen we door het documenteren van het incident response proces samen met de klant doornemen wat beter kan en wat goed ging. Hiermee kunnen we ons eigen proces verbeteren en die van de klant.

A.5.28 · BEWIJSMATERIAAL

Als een incident leidt tot juridische stappen of een formele melding, moet bewijsmateriaal op een forensisch verantwoorde manier verzameld en bewaard zijn.

Peakproteqt: Zelf voeren wij geen forensisch onderzoek uit indien dit toch nodig blijkt te zijn na een cyberincident. Wel hebben we hiervoor goede samenwerkingen met partijen uit Nederland die dit wel kunnen. De reden dat wij dit niet doen komt door technische complexiteit die bij forensisch onderzoek komt kijken.

A.6.8 · RAPPORTAGE

Medewerkers moeten een manier hebben om vermoedens van beveiligingsincidenten te melden, en dit moet laagdrempelig zijn.

Peakproteqt: Onze klanten krijgen naast het incident response plan ook de mogelijkheid om cyberincidenten direct bij ons te melden op een laagdrempelige manier. Zo houden we de lijnen kort en weten de medewerkers van onze klanten waar ze aan toe zijn.