Statement Cyber Security

Onze maatschappij wordt steeds afhankelijker van digitale processen, vooral als gevolg van de verdere digitalisering van de bedrijfsvoering. Het kunnen terugvallen op analoge uitwijkmogelijkheden is steeds minder aan de orde. Samen met de digitalisering zien we de afgelopen jaren een significante toename in cybercrime-incidenten. Dit blijkt uit het jaarlijkse Cybersecuritybeeld Nederland (CSBN), dat het Nationaal Cyber Security Centrum (NCSC) in samenwerking met de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) heeft opgesteld. In alle landen waar Simac aanwezig is, zien we een vergelijkbaar beeld.
Overheidsinstanties waarschuwen ook dat cybercriminelen steeds vaker nauwe banden met regeringen van bepaalde landen hebben, zoals ook eerder dit jaar door de NCTV omschreven in het Dreigingsbeeld Statelijke Actoren. Andere oorzaken van maatschappij ontwrichtende omstandigheden zijn ransomware afkomstig van criminelen en digitale uitval veroorzaakt door natuurlijke of technische storingen; recentelijk neemt de geopolitieke dreiging sterk toe.

Weerbaar

Cyberincidenten kunnen onze diensten en die van onze klanten in het hart raken en gedurende korte of lange tijd verlammen. We besteden daarom al sinds jaar en dag continu aandacht aan onze digitale weerbaarheid. De afgelopen jaren hebben we continu extra stappen gezet om deze weerbaarheid structureel te vergroten. De permanente dreiging van zowel buitenlandse regeringen als cybercriminelen blijft onverminderd groot. We beschermen ons netwerk met een in-depth verdedigingssysteem om kwaadwillenden te bestrijden en succesvolle ransomware-aanvallen te voorkomen. Onze verdediging betreft zowel organisatorische, procesmatige als technische maatregelen.

Risicoanalyse

We hebben de vitale processen geïdentificeerd voor onze organisatie (BIA) en voeren methodologisch dreigingenanalyses uit (RIA), waarbij we passende en evenredige maatregelen implementeren om kwetsbaarheden te verminderen.

Het Simac Security Operating Center

Getroffen maatregelen

Als directie nemen we informatiebeveiliging en privacy zeer serieus en onderhouden we een actief beleid in deze. We worden in de uitvoering van het beveiligingsbeleid geholpen door onze nauwe contacten met leveranciers, belangengroepen (zoals het NCSC en CWB), cybercrimeverzekeraars, ons eigen Security Operating Center (SOC) en ons ISMS (dat we volgens internationale normen certificeren, zoals ISO27001, ISO27701, NEN7510 en ISAE3402 type II).

We hebben een bestuursmodel ingericht waarbij we in crisissituaties snel kunnen escaleren en direct kunnen reageren op cybersecurityincidenten. Een security awareness programma zorgt daarnaast voor blijvend bijschaven van de alertheid en kennis van onze medewerkers om cybersecurityincidenten te voorkomen of herkennen.

Incident respons-processen, escalatieprocedures, calamiteitenplannen en een business continuity proces zijn in de organisatie geborgd, en worden regelmatig geoefend.

Met de implementatie van de NIS2-richtlijn nemen wij onze verantwoordelijkheid om de netwerk- en informatiebeveiliging op het gewenste niveau te houden. We hebben onze cyberbeveiligingsstrategie en maatregelenprogramma aangepast om te voldoen aan de strengere eisen van de NIS2 richtlijn.

Maartje van Schagen
ceo