Statement Cyber Security

Our society is becoming increasingly dependent on digital processes, especially as a result of the further digitalization of business operations. Being able to fall back on analog fallback options is becoming less and less of an issue. Along with digitization, we have seen a significant increase in cybercrime incidents in recent years. This is evident from the annual Cyber Security Assessment Netherlands (CSBN), which the National Cyber Security Centre (NCSC) has drawn up in collaboration with the National Coordinator for Counterterrorism and Security (NCTV). In the other countries where Simac has a presence, we see a similar picture. These government agencies are also warning that cybercriminals increasingly have close ties to governments of countries, as also described by the NCTV earlier this year in the State Actors Threat Assessment. Other causes of society-disrupting conditions include ransomware originating from criminals and digital outages caused by natural or technical failures; recently, the geopolitical threat is increasing sharply.

Resilient

Cyber incidents can strike at the heart of our services and those of our customers, paralyzing them for short or long periods of time. We have therefore been paying continuous attention to our digital resilience for many years. In recent years, we have taken extra steps to structurally increase this resilience. The permanent threat from both foreign governments and cybercriminals remains as great as ever. We protect our network with an in-depth defense system to combat malicious parties and prevent successful ransomware attacks. We continually update these measures. Our defenses include organizational, process and technical measures.

Het Simac Security Operating Center

Measures taken

As management, we take information security and privacy very seriously and maintain an active policy in this regard. We are assisted in implementing the security policy by our close contacts with suppliers, interest groups (such as the NCSC and CWB), cybercrime insurer, our own Security Operating Center (SOC) and our ISMS (which we certify according to international standards, such as ISO27001, NEN7510 and ISAE3402 type II).

We have set up a governance that allows us to escalate quickly in crisis situations and respond immediately to cybersecurity incidents. A security awareness program also ensures that our employees' alertness and knowledge are continually honed in order to prevent or recognize cybersecurity incidents.

Incident response processes, escalation procedures, contingency plans and a business continuity process are secured in the organization, and are regularly practiced.

Risk Analysis

We have identified the vital processes for our organization (BIA) and conduct methodological threat assessments (RIA), selecting and implementing the most effective and efficient measures to mitigate any vulnerabilities.

Eric van Schagen
ceo